CITY OF CHARLES TOWN
CITY COUNCIL
AGENDA • OCTOBER 19, 2026

Regular Session **COUNCIL CHAMBERS** **7:00 PM**
****UPDATED AGENDA****
101 E Washington Street, Charles Town, WV 25414

CALL TO ORDER

1. MOMENT OF SILENCE AND PLEDGE OF ALLEGIANCE

2. APPROVAL OF MINUTES

: **2026-2038:** City Council Meeting Minutes - October 5, 2026
City Council Meeting Minutes - October 5, 2026 Draft.pdf

3. PUBLIC COMMENT

4. WARD REPORTS

5. MAYOR'S REPORT

6. COMMITTEE REPORTS

: **2026-2039:** Board of Parks and Recreation Commission Meeting - October 8, 2026
September_2026_Meeting_Minutes.pdf

: **2026-2042:** Ordinance Committee Meeting - October 15, 2026

7. CITY MANAGER REPORT

: **2026-2043:** City Manager's Report - October 19, 2025
Council - October 19, 2026.docx
CTUB Handout - JCC Workshop - Impacts of Growth on Municipal Utilities (FINAL).pdf

8. POLICE CHIEF REPORT

9. UNFINISHED BUSINESS

: **2026-2044:** Community Grant Policy Review
Revised Community Funding Policy_v2.pdf

: **2026-2045:** Cloud Data Storage Discussion
Tek Advisors PremisevsCloud Summary.pdf
Q_A Council Questions.pdf
Motorola QUOTE - 3745884 - Charles Town - Cloud Migration 08212026.pdf
Motorola QUOTE - 3805219 - Charles Town - (19) V700.pdf
Motorola QUOTE - 3844710 - Charles Town - Deployment.pdf
Axon Charles Town Police Department - WV_Q-917596.pdf
Axon Charles Town Police Department - WV_Q-964558.pdf

Axon Charles_Town_PD_Value_Brief_Q-917596-001.pdf
Axon_print_productcards_onepagers_axonassistantonepager_8-5x11_03b-2.pdf
Axon 2e0a6a4d-02c4-435f-8dba-559c01651219.pdf
Axon 007.URCS_AxonFleet3.RespondProductCard_FNL.indd.pdf
Axon Body 4 Product Card EN_US.pdf
CaseGuard Charles Town Police Department 1 Ultimate Suite_V1.pdf
CaseGuard_Studio_Hardware_Recommendations (1).pdf
Estimate_1572_from_Executive_Emergency_Lighting_LLC.pdf
CJIS_Security_Policy_v6-0_20241227 (1).pdf

: **2026-2054:** Good Neighbor Data Center Guidelines
Governor Letter Data Centers.pdf
Data Center Guardrails.pdf

: **2026-2055:** Depot Land Memorandum of Understanding (MOU) with Charles Town Parks and Recreation Commission
Depot District Memorandum of Understanding_Draft 2.pdf

10. NEW BUSINESS

: **2026-2008:** TXA2026-01 - Flood Control Ordinance - First Read
1. Report.pdf
Floodplain Resolution Draft.pdf

: **2026-1989:** Walkability Improvement Grant - Updates
1. Staff Report.pdf
2. WIP Application- CURRENT.pdf
3. WIP Application- DRAFT Version with changes.pdf

: Facade Improvement Grant - Updates
1. Staff Report.pdf
2. FIP Application- CURRENT.pdf
3. FIP Application- DRAFT Version with changes.pdf

: **2026-2046:** Updated Opioid Fund Resolution
Updated Grant Funds Resolution.pdf
2025-005 - Resolution Allocating Opioid Funds to Police Social Work Program.pdf

: **2026-2047:** City Service Fee on New Construction Discussion - Possible Executive Session
Developer Fee Council Packet.pdf
FINAL REPORT.pdf
Subdivision Proffers.pdf
W Va Code 8-13-13.pdf
Ranson City Service fee 1.docx

: **2026-2048:** FY2027 General Fund Budget Revision #3
FY 2027 GF Revision #3.pdf

: **2026-2049:** FY2027 Capital Fund Budget Revision #2
FY 2027 Capital Budget 2nd Revision.pdf

: **2026-2050:** Vacant Structure Building Registry Appeal - Vacant Structures Code Exemption Procedures Policy

Vacant Structure Code Exemption Procedures Final.pdf

: **2026-2052:** Greenway Engineering Study - Watershed 3 Next Steps
7037.07P2 CCT Watershed 3 Pt 2-3 Proposal 101326 - GE Signed.pdf
Watershed 3 Greenway Stormwater.pdf

11. REFERRALS TO COMMITTEES/COMMISSIONS

12. APPROVAL OF BILLS

: **2026-2051:** Payment of Bills - October 19, 2026
PARKS N REC COUNCIL REPORT 2026-10-19.pdf
COUNCIL REPORT PCARD 10-19-2026.pdf
GEN FUND COUNCIL REPORT 2026-10-19.pdf
CAPITAL RESERVE COUNCIL REPORT 2026-10-19.pdf

13. ADJOURNMENT

14. INFORMATION ONLY - NEXT MEETING, Monday, November 2, 2026, at 7:00PM

: **2026-2061:** An Ordinance to Approve the July 2026 Replacement Pages to the Codified Ordinance
Ordinance to Approve the July 2026 Replacement Pages - signed.pdf

: **2026-2062:** Oath of Office - Thomas Mitchell Board of Parks and Recreation Commission
Thomas Mitchell Oath - 10-7-26.pdf

: **2026-2063:** Infrastructure Committee Report - October 1, 2026
Report_ Infrastructure October 1, 2026.pdf

: **2026-2064:** 2026-008 Resolution on Transmission Line Projects
2026-008 - Resolution on Transmission Line Projects.pdf

15. NOTICE: The Public May View the Meeting Live by Clicking on the Event Link at:

https://www.charlestownwv.us/government/agendas_minutes.php

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2038: City Council Meeting Minutes - October 5, 2026

ATTACHMENTS:

- City Council Meeting Minutes - October 5, 2026 Draft.pdf

CITY OF CHARLES TOWN

CITY COUNCIL

MINUTES • October 5, 2026

Regular Meeting **Council Chambers** **7:00 PM**

101 East Washington Street, Charles Town, WV 25414

CALL TO ORDER

Attendee Name	Title	Status	Arrived
Micheal George	Mayor	Present	
James Kratovil	Councilmember	Present	
Elizabeth Ricketts	Councilmember	Present	
Jeff Hynes	Councilmember	Present	
Kevin Tester	Councilmember	Present	
Nate Hartman	Councilmember	Present	
Alden Roth	Councilmember	Present	
Julie Smith	Councilmember	Present	
Andie Sugrue	Councilmember	Present	

Ms. Alissa Meeks, Interim City Manager; Ms. Stephanie Grove, City Attorney; Ms. Lori Nice, Finance Director; Mr. James Newman, City Planner; Ms. Roberta Meade-Curry, Long-Range Planner; Mr. Stephen Galleher, Operations Director; and Lieutenant Quinnam, Charles Town Police Department (CTPD) were also in attendance.

1. MOMENT OF SILENCE AND PLEDGE OF ALLEGIANCE

2. APPROVAL OF MINUTES

2026-1966: City Council Meeting Minutes - September 21, 2026

The following change was made to the September 21, 2026, meeting minutes.

Packet Page 7, Agenda Item 2026-1936: Parks and Recreation Department Transfer to Move from Community Development Division to Operations Division: Rewrite the motion to state, **"Mr. Hynes motioned to move the Parks and Recreation Manager position under the Operations Division and appoint the Operations Director as the Director of Parks and Recreation with the understanding that this can be revisited when a new city manager is hired."**

3. PUBLIC COMMENT

Ms. Nicola Bastian spoke on her concerns with House Bill 2014 and why she thinks it's unconstitutional.

4. WARD REPORTS

Ward 1

Mr. Kratovil had nothing to report.

DRAFT

Ms. Ricketts reported that she attended the statewide training on emergency preparedness and the state auditor's training.

Ward 2

Mr. Hynes had nothing to report.

Mr. Tester reported that he volunteered at Ms. Willa's Bookstore event and would like to see more of these types of events in Charles Town. He also attended the data center summit at the Jefferson County Commissioner's meeting room.

Mr. Hynes had nothing to report.

Ward 3

Mr. Hartman had nothing to report.

Mr. Roth reported that he attended the ribbon cutting ceremony for the Chet Hines Bridge at Happy Retreat and reminded everyone that there are several trails on the grounds open to the public which lead to the bridge that connects to the Washington family's gravesite.

Ward 4

Ms. Sugrue reported that she volunteered at Ms. Willa's Bookstore event and thanked everyone involved for all their hard work in making the event a success.

Ms. Smith reported that it was wonderful to see so many people downtown for Ms. Willa's Bookstore event.

5. MAYOR'S REPORT

Mayor George reported that he attended Charles Town Utility Board (CTUB) meetings, the data center summit, Region 9 meeting for grant writing, the bridge dedication, and Ms. Willa's Bookstore event.

6. COMMITTEE REPORTS

2026-1967: Ordinance Committee Report - September 17, 2026

Mr. Tester gave an oral report.

2026-1980: Infrastructure Committee Report - October 1, 2026

Ms. Ricketts reviewed the Infrastructure Committee report.

7. CITY MANAGER REPORT

2026-1968: City Manager's Report - October 5, 2026

Ms. Meeks reviewed the city manager's report.

8. POLICE CHIEF REPORT

There was no police report.

9. UNFINISHED BUSINESS

2026-1969: Cloud Data Storage Discussion

Mr. Hynes moved to remove this agenda item from the Table. Mr. Hartman seconded the motion, and it passed by a 6-3 vote. Mayor George declared the agenda item off the Table.

DRAFT

RESULT:	**APPROVED [6-3]**
MOVER:	Jeff Hynes
SECONDER:	Nathanael Hartman
AYES:	George, Hynes, Tester, Hartman, Smith, Sugrue
NAYS:	Kratovil, Ricketts, Roth

Mr. Hartman moved to Table this agenda item until the October 19, 2026, council meeting. Mr. Roth seconded the motion, and it passed by a 7-2 vote.

RESULT:	**APPROVED [7-2]**
MOVER:	Nathanael Hartman
SECONDER:	Alden Roth
AYES:	Kratovil, Ricketts, Hynes, Hartman, Roth, Smith, Sugrue
NAYS:	George, Tester

2026-1970: Jefferson County Commission's Housing Summit - Discussion on Participating

After discussion it was decided that the city would not participate in the Jefferson County Commission's housing summit. A statistical fact sheet will be developed by staff to show growth within the city and why development should be within city limits.

10. NEW BUSINESS

2026-1937: Updating the Flood Control Ordinance

Mr. Hynes moved to direct staff to advertise a public hearing on the flood control ordinance for the October 21, 2026, council meeting. Mr. Hartman seconded the motion, and it passed by unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jeff Hynes
SECONDER:	Nathanael Hartman
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

2026-1965: Huntfield Proffer Review

Mr. Tester moved to enter into Executive Session to receive legal advice. Mr. Hynes seconded the motion, and it passed by unanimous vote. Mayor George declared the council in Executive Session.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Kevin Tester
SECONDER:	Nathanael Hartman
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

Mayor George declared the council out of Executive Session.

Mr. Hynes moved to inform the Charles Town Planning Commission that the council believes the Dan Ryan application as submitted is substantially

DRAFT

in compliance with Proffer #1 Education on the Huntfield list of proffers for Proffer Amendment #3 approved on August 19, 2024. Mr. Hartman seconded the motion, and it passed by unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jeff Hynes
SECONDER:	Nathanael Hartman
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

2026-1972: Board of Parks and Recreation Commission Appointment

Mr. Kratovil moved to appoint Mr. Thomas Mitchell to the Board of Parks and Recreation Commission for a partial term ending June 1, 2027. Mr. Roth seconded the motion, and it passed by unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	James Kratovil
SECONDER:	Alden Roth
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

2026-1973: An Ordinance to Approve the July 2026 Replacement Pages to the Codified Ordinances

Mr. Kratovil moved to approve the Ordinance to Approve the July 2026 Replacement Pages to the Codified Ordinances. Mr. Tester seconded the motion, and it passed by unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	James Kratovil
SECONDER:	Kevin Tester
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

2026-1981: Davenport Street Extension Proposal

City staff will look into options on how/if the remaining section of Davenport Street can be paved and bring those back to the council at a later date.

2026-1982: Crosswalk Discussion and Referral

Mr. Hynes moved to have the Infrastructure Committee work with city staff to develop a crosswalk policy. Mr. Hartman seconded the motion, and it passed by unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jeff Hynes
SECONDER:	Nathaneal Hartman
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

2026-1983: A Resolution of the City Council of Charles Town, West Virginia Opposing the Valley Link North, Gore-Doubs-Goose Creek, and Mid-Atlantic Resiliency Link (MARL) Transmission Line Projects

DRAFT

Mr. Hynes moved to direct the mayor to update the 2025-007 Resolution to include the Mid-Atlantic Resiliency Link (MARL), the Valley Link North, and the Gore-Doubs-Goose Creek Link and send out to Ms. Melissa Hope and the Public Service Commission of WV. Mr. Kratovil seconded the motion, and it passed by a unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jeff Hynes
SECONDER:	James Kratovil
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

2026-1984: Good Neighbor Data Center Guidelines

Mr. Hartman moved to direct the mayor and staff to compose a letter to the WV governor regarding House Bills 2014, including the guardrails the city feels are important, how local authorities should have more control in the decision-making process and receive a higher percentage of tax revenue. Mr. Roth seconded the motion, and it passed by unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Nathanael Hartman
SECONDER:	Alden Roth
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

2026-1985: Opioid Funds Discussion

Ms. Margaret Kursey of the Martinsburg Initiative reported that they have received a 4-year Mobile Crisis Integrated Grant that will fund the Charles Town police support specialist beginning in October of 2026. Ms. Grove will rewrite the "2025-007- Resolution Allocating Opioid Funds to Police Social Work Program" to allocate the unspent $46,000 for FY2027 to the Charles Town Initiative and bring it back to council. The remaining opioid funds will need to be allocated in the next upcoming fiscal years.

11. REFERRALS TO COMMITTEES/COMMISSIONS

2026-1956: Facade Improvement Grant - Referral to Ordinance Committee

Council directed staff to make the necessary policy changes and bring it back to council.

12. APPROVAL OF BILLS

2026-1988: Payment of Bills - October 5, 2026

Mr. Kratovil moved to approve the bills for payment. Mr. Hartman seconded the motion, and it passed by unanimous vote.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	James Kratovil
SECONDER:	Nathaneal Hartman
AYES:	George, Kratovil, Ricketts, Hynes, Tester, Hartman, Roth, Smith, Sugrue

DRAFT

13. ADJOURNMENT

Mayor George asked if there was any other business to come before the council. Hearing none, he adjourned the meeting.

14. INFORMATION ONLY - NEXT MEETING, Monday, October 19, 2026, at 7:00PM

2026-1974: Appeal to the Facade Improvement Grant Letter

2026-1975: Personnel Committee Report - September 14, 2026

2026-1976: Parks and Recreation Expense Approval Report - September 21, 2026

2026-1977: Charles Town Utility Board Meeting Minutes - July 8, 2026, July 22, 2026, and August 26, 2026

2026-1978: Daniel Shirkey Oath of Office - BZA

2026-1979: Colin Stine Public Comment Letter

15. NOTICE: The Public May View the Meeting Live by Clicking on the Event Link at: https://www.charlestownwv.us/government/agendas_minutes.php

DRAFT

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2039: Board of Parks and Recreation Commission Meeting - October 8, 2026

ATTACHMENTS:

- September_2026_Meeting_Minutes.pdf

City of Charles Town

Parks and Recreation Commission Report

September 10, 2026 / 6:00 PM / City Hall

I. CALL TO ORDER: 6:01 PM

Persons Present:

Commissioners Present: Alden Roth, Thrudy Roth, Elizabeth Ricketts, Nick Zaglifa (Remote)

Staff: Gavin Bailey

Guests: Tammy Connors, Meridith Marshall

II. APPROVAL OF MINUTES:

The Commission considered approval of the minutes from the August 13, 2026 regular meeting and the August 20, 2026 special meeting.

Motioned: A. Roth, hearing no objection approved- *Unanimous*

III. UNFINISHED BUSINESS

2026-1893 Charles Town Public Pool Splash Pad Update

Staff reported that splash pad construction will commence soon. Snow guards were installed on the roof last week. Staff will provide additional information as it becomes available.

No Action.

2026-1894 Pool Operations Discussion

Staff presented an estimate from TechStar and is obtaining an additional estimate from MS Johnson, the contractor that worked on the HVAC unit in the lifeguard lounge. Preliminary assessment indicates a separate, larger unit than the lifeguard lounge unit may be required. Sizing considerations include the windows, five compressor units (two refrigerators, one freezer, one ice cream machine, and one slushie machine), and two heating elements (one hot holder and one hotdog roller).

The board also discussed the end of season bonuses for all pool staff.

Motion: Approve end of season bonus for all pool staff members regardless of calculated hours.

Motioned: E. Ricketts, 2nd: T. Roth

Unanimous

2026-1895 CLEAN Parks Initiative

Staff reported that the RFP has been distributed to firms and is being advertised, with a submittal deadline of September 16th. The project has been granted an extension to April 30, 2027, with significant flexibility on deliverables. All parties must be paid by April 30, 2027, and must meet certain deliverables by that date; however, the City has discretion over those deliverables, and work may continue afterward.

No Action.

2026-1896 Insurance Requirements for Events at Happy Retreat

Staff reported that the current certificate of insurance (COI) section of the MOU states only that the City will coordinate with Happy Retreat. Staff was directed to coordinate with the Friends of Happy Retreat to include the City of Charles Town as being one of the insured parties in their insurance requirements for renters and vendors.

No Action.

2026-1896 Parks Master Plan Discussion

The RFP was added to the agenda packet. It was reported that the Depot District will be under the management of Parks and Rec.

No Action.

IV. NEW BUSINESS

2026-1898 Additional Lighting at Pickleball and Basketball Courts

Staff reported that some companies declined the job as outside their scope of work or too small. Two estimates were received: one from FSG (turnkey, including supplies and installation) and one from Brite Court (materials only, installation not included). More estimates are being made and staff will return with updates.

Motion: to table item until there are additional quotes.

Motioned: E. Ricketts, 2nd N. Zaglifa

Aye: E. Ricketts, N. Zaglifa, T. Roth

Nay: A. Roth

Passed

2026-1899 Native Plants at Pickleball Courts

A diagram from Tree Board president Aaron Amore was included for the Commission's consideration around the new pickleball court at Jefferson Memorial Park. First Energy might have a grant to support

Motion: to forward to Charles Town Tree Board for consideration and to seek grant funding.

Motioned: E. Ricketts, 2nd: N. Zaglifa

Unanimous

2026-1900 Selection of CLEAN Parks RFP Evaluation Panel

The Commission discussed the selection of an evaluation panel for the CLEAN Parks RFP.

Motion: to form a selection committee with the following members pending their willingness to be involved: Elizabeth Ricketts, Kevin Derr, Alden Roth, and John Maxey, with alternative member Jamila Jones.

Motioned: E. Ricketts, 2nd: N. Zaglifa

CLEAN Parks RFP Optional Scope Funding

The Commission discussed optional scope funding for the CLEAN Parks RFP.

No Action.

2026-1901 Authorization of Spokesperson for RFP Negotiations

The Commission discussed authorizing a spokesperson for RFP negotiations.

Motion: to Nominate Alden Roth as the committee spokesperson for the CLEAN Parks RFP evaluation panel.

Motioned: E. Ricketts, 2nd: T. Roth

Unanimous

2026-1902 Tree Maintenance RFP Discussion

The Commission reviewed a survey conducted by maintenance director Jim Wysong and board president Alden Roth, a map of the survey for Jefferson Memorial Park, and a prior survey conducted by Viking with an estimate for tree removal.

Motion: authorize staff to utilize $9,999 from parks and recreation capital outlay for the removal of the 2 or 3 trees of most concern around the pool.

Motion: E. Ricketts, 2nd: T. Roth

Unanimous

2026-1903 Fall Junior Tennis and MOU Review

The Commission reviewed the Junior Tennis MOU. The director of Junior tennis is currently holding informal meetings at the park, acting outside of the league with no monetary support or ability to reserve courts.

> Motion: to waive the fall junior tennis registration fee for fall 2026 with the understanding that the city of Charles Town will not make any purchases on the league's behalf.
>
> Motioned: E. Ricketts, 2nd N. Zaglifa
>
> *Unanimous*

2026-1904 Use of Pool by the Swim Team in 2027

Members of the Swim Team Tammy Connors and Meridith Marshall came in for comment about the use of the pool by the Jeferson Memorial Park Dolphins Swim Team. They stressed the teams history and the demand that exists for specifically summer swimming programs in the area. They are open to discussing scheduling for swim team practices and further discussion will be held at a later time.

> *No action.*

2026-1905 Recommended Parkland Language for Citywide Zoning Rewrite

Document was provided as a table drop.

> Motion: to table.
> Motioned: E. Ricketts, 2nd: A. Roth
> Aye: E. Ricketts, A. Roth, T. Roth
> Nay: N. Zaglifa
> *Passed*

2026-1906 MANAGER'S REPORT

Staff provided updates in a report seen in the agenda packet. Of note is the scheduling of a bridge dedication event at Happy Retreat Park.

> Motion: to have the Friends of Happy Retreat decide the best date.
>
> Motioned: A. Roth, 2nd: T. Roth
>
> *Unanimous*

The parks manager also informed the board that he has provided his two-week notice to the city and will be resigning in the 4th week of September.

2026-1907: Park Updates

None.

VI. ADJOURNMENT: 8:04 PM

VII. NEXT MEETING: City Hall - October 8th, 2026 at 6pm

2026-2042: Ordinance Committee Meeting - October 15, 2026

ATTACHMENTS:

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2043: City Manager's Report - October 19, 2025

ATTACHMENTS:

- Council - October 19, 2026.docx
- CTUB Handout - JCC Workshop - Impacts of Growth on Municipal Utilities (FINAL).pdf

City of Charles Town

101 East Washington Street, P.O. Box 14, Charles Town, WV 25414
Phone: (304) 725-2311 ♦ Web: www.charlestownwv.us

MEMORANDUM TO THE MAYOR AND CITY COUNCIL

FROM: Alissa Meeks, Interim City Manager
SUBJECT: City Manager's Report
DATE: October 19, 2026

This report is designed to provide information on substantive issues and meaningful project updates on items of importance to the Mayor and City Council.

ADMINISTRATION, MAINTENANCE, AND OPERATIONS

City Manager RFP Search Firm Proposals: The City received seven (7) firm submissions, and the Personnel Committee will be reviewing those responses and selecting the top 3 firms for interview consideration.

Parks and Recreation Applications: Operations received 23 applications for the Parks and Recreation Manager position. Staff is currently reviewing those applications and will be scheduling interviews in the subsequent weeks.

CLEAN Parks Initiative: Stromberg Garrigan & Associates (SGA)/Alpha has been identified as the "top-scoring" firm in the Clean Parks RFP. The negotiations team will work to finalize a cost proposal for the overall project.

Charles Town Utility Board Handout – Attached to this report is a handout drafted by CTUB Manager, Paul Mantello, with associated building permit data, outlining projected capacity levels and the importance of regional planning efforts.

COMMUNITY AND ECONOMIC DEVELOPMENT

Augustine Trail: Equipment has been mobilized and is on-site as Phase 2 is underway for construction.

Ribbon Cutting: Please join us at 301 W. Washington Street as we celebrate a Grand Opening ribbon-cutting for Wilder Bakehouse on November 7th at 10AM.

Walks about Nothing – Christmas Lights Edition: On October 21st "Walks" participants will be helping our Public's Works team manually screw in thousands of Christmas light bulbs for the City's new Christmas lights installation. Bring Christmas cookies, your holiday spirit, and a few helping hands to join us in the fun.

Long Range Planner – The vacant position is currently being advertised on multiple platforms.

HEPMPO Regional Safety Study Survey: The survey seeks ranking the region's top priority intersections, identifying locations of safety concerns, suggestions and improvements. The survey closes on November 15th and is available online at: https://live.metroquestsurvey.com/?u=ge5q5p#!/.

Customer Growth: July 2021 – September 2026

Fiscal Year	Water Customers	Sewer Customers
FY 2021	6,315	8,053
FY 2022	6,428	8,232
FY 2023	6,612	8,477
FY 2024	7,030	9,090
FY 2025	7,473	10,061
FY 2021 – FY 2025 Growth Rate	+1,158 (+18.3%)	+2,008 (+24.9%)
September 2026 (Current)	7,889	11,170
Jul. 2025 – Sep. 2026 Growth Rate	+416 (+5.6%)	+1,109 (+11.0%)
Jul. 2021 – Sep. 2026 Growth Rate	+1,574 (+24.9%)	+3,117 (+38.7%)

Notes: Customer Counts from FY2021–FY2025 CTUB Annual Audits; September 2026 data provided by CTUB Administrative Staff.

Operating Performance: FY 2021 – FY 2025

Fiscal Year	Revenue	Expenses	Operating Income
FY 2021	$10.2M	$8.8M	$1.4M
FY 2022	$10.2M	$8.6M	$1.6M
FY 2023	$10.6M	$9.8M	$0.8M
FY 2024	$11.7M	$10.6M	$1.1M
FY 2025	$12.8M	$12.5M	$0.3M
FY 2021 – FY 2025 Growth Rate	+$2.6M (+25.5%)	+$3.7M (+42.0%)	

Notes: Financial Data from FY2021–FY2025 CTUB Annual Audits; Operating income narrowed from approximately $1.4 million to $0.3 million, but do not establish that growth caused the expense increase; rates, inflation, labor, energy, maintenance, and depreciation.

Infrastructure Investment & Financing: FY 2021 – FY 2025

Fiscal Year	Net Capital Assets	Long-Term Debt	Capital Contributions (60% CIF)
FY 2021	$74.8M	$40.2M	$1.8M
FY 2022	$74.7M	$38.5M	$3.9M
FY 2023	$79.8M	$43.6M	$6.5M
FY 2024	$84.1M	$41.4M	$7.3M
FY 2025	$84.9M	$39.5M	$5.8M

Notes: Financial Data from FY2021–FY2025 CTUB Annual Audits; Approximately $25.3 million in total capital contributions over five years, with an average 60% coming from Capacity Improvement Fee (CIF), and remaining as contributed infrastructure, grants, and other Capital Assets increased about $10.1 million (+13.5%).

Treatment Capacity & Growth Readiness: CY 2025 Average Flows

Facility	Design (MGD)	Average (MGD)	Remaining (MGD)	Utilization
Charles Town Water Treatment Plant	2.80	1.646	1.154	58.8%
Charles Town Wastewater Treatment Plant	1.75	1.179	0.571	67.4%
Tuscawilla Wastewater Treatment Plant	0.50	0.183	0.317	36.7%

Notes: The Charles Town Water Plant's 2025 average flow represents approximately 58.8% of its 2.8 MGD design capacity; the Charles Town Wastewater Plant operated at approximately 67.4% of its 1.75 MGD design capacity. Tuscawilla averaged approximately 36.7% of its 0.5 MGD design capacity. These figures do not consider whether necessary conveyance, storage, pumping, or peak-flow capacity exists at a proposed development location.

Municipal & County Building Permits: August 2021 – Present

Locality	Buildings Permits (Last 5 Years)
City of Charles Town	1,011
City of Ranson	1,734
Jefferson County	1,562
TOTAL	4,307

Projected Customer Growth: 2026 – 2040

Year	Water Customers	Sewer Customers
2026 (Current)	7,889	11,170
2030 (Projected)	9,336	13,955
2035 (Projected)	11,522	18,433
2040 (Projected)	14,222	24,347
2026 – 2040 Growth	**+6,333 (+80.3%)**	**+13,177 (+118.0%)**

Notes: Projections based on FY2021–FY2025 compound annual customer growth rates of approximately 4.3% for water and 5.7% for wastewater.

Treatment Capacity & Growth Readiness: Projected 80% & 100% Thresholds

Facility	2025 Average	80% Threshold	Projected 80% Year	Projected 100% Year
Charles Town Water Treatment Plant	1.65 MGD	2.24 MGD	2032–2033	2037–2038
Combined Wastewater Treatment Plants	1.36 MGD	1.80 MGD	2030	2034
Charles Town Wastewater Treatment Plant	1.18 MGD	1.40 MGD	2028	2032

Notes: Projections apply FY2021–FY2025 customer growth rates to CY2025 average treatment flows. The 80% threshold is a planning benchmark, not a regulatory capacity limit. NPDES Permitting requires planning and design commence at 90%.

Growth in Jefferson County

- Economies of Scale & Rate Stabilization: Additional connections spread fixed costs over more customers, but may require increased incremental costs associated with treatment, pumping, collection, distribution, storage, and fire-flow improvements. It's important to note that customer growth alone does not guarantee lower operating costs.

  While growth provides opportunities to distribute existing fixed expenses across a larger customer base, inflation, increased maintenance and staffing, and changing regulatory requirements can often offset those benefits. Carefully ensuring "growth pays for growth" is critical for offsetting incremental costs and creating ratepayer benefits from economies of scale.

- Available Capacity by Location & Peak Demand: If growth is to create economic and ratepayer benefits, infrastructure capacity must be evaluated by location and peak demand, and not only by systemwide permitted treatment capacity. Although CTUB's water and wastewater treatment facilities may have available capacity based on average daily flows, that capacity is not necessarily available or accessible throughout the service territory.

  The ability to accommodate new development depends on the capacity and condition of the infrastructure serving the proposed location, including water transmission and distribution mains, storage facilities, pumping stations, wastewater collection systems, and forcemains. Water service must also satisfy peak demand, pressure, and fire protection requirements, while wastewater infrastructure must accommodate peak hydraulic loading and wet-weather infiltration and inflow. For example, a proposed subdivision could generate wastewater flows within treatment and pumping capacities, but its connection might also be limited by undersized or outdated downstream infrastructure. Consequently, two developments with similar projected demands may have substantially different infrastructure requirements and costs depending on their location.

  Again, ensuring "growth pays for growth" and identifying necessary improvements before development occurs, to ensure that growth-related infrastructure costs are appropriately allocated, is critical for creating and realizing the potential local benefits of growth.

- Regional Infrastructure Planning and Intergovernmental Coordination: Coordination between local and state government agencies is critical to ensure that development, infrastructure investment, and public funding decisions are well coordinated, so that growth is accommodated efficiently, existing customers are protected from disproportionate financial burdens, and infrastructure investments provide the greatest possible long-term community benefit.

- Projected Growth & Utility Capacity Planning: Based on CTUB's customer growth rates between FY2021 and FY2025, water customers increased at an average annual rate of approximately 4.3%, while wastewater customers increased approximately 5.7% annually.

  If future treatment demands increase proportionally with historical customer growth, the Charles Town Wastewater Treatment Plant could reach approximately 80% of its 1.75 MGD design capacity, around 2028, with the combined wastewater treatment system, including the Tuscawilla Plant, reaching that threshold around 2030. The Charles Town Water Treatment Plant could reach approximately 80% of its 2.80 MGD design capacity around 2032.

  These projections highlight the importance of beginning infrastructure planning well before treatment facilities approach their design capacities. Given the time required for engineering, regulatory approvals, financing, and construction, coordinated regional planning is essential to ensure that utility infrastructure keeps pace with development.

  CTUB recommends that regional development forecasting and infrastructure planning be coordinated across jurisdictions to identify future capacity needs early, facilitate timely infrastructure investments, and ensure that growth-related improvements are appropriately funded without disproportionately burdening existing utility customers.

Paul Mantello, General Manager
Charles Town Utility Board
301-473-3123 (Cell)
pmantello@ctubwv.com

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2044: Community Grant Policy Review

This agenda item was Tabled at the September 21, 2026, city council meeting.

ATTACHMENTS:

- Revised Community Funding Policy_v2.pdf

COMMUNITY PROMOTION FUNDING POLICY

Proposed revised policy — for City Council consideration

Purpose:

The purpose of this Policy is to establish a process for distribution of the City of Charles Town Community Promotion funds, previously referred to as "but for" funds. This policy is designed to assist with proper fiscal planning and the promulgation of clear guidelines for prospective recipients of City funds.

Scope and Effective Date:

This Policy shall cover all Community Promotion funding beginning with FY 2026 and annually thereafter. Organizations or Departments that receive funding through a dedicated regular line item in the budget are not eligible for Community Promotion Grants. The City will divide Community Promotion funding into two separate grant categories: Community Partnership Grants and Community Grants.

General:

The City, in its sole discretion, may provide funding or grants to nonprofit, charitable or civic organizations in order to supplement existing funds that either create or enhance services that positively impact the greatest number of City residents. It is the intent of these guidelines to provide that any funds appropriated shall be used to promote the general welfare of the residents of the City with priority given to the Community Partnership category of grants. Priority areas are determined by the City Council and Mayor and may be reevaluated annually. Any funds appropriated under the provisions of this Policy shall be used and expended under the direction and control of Treasurer as determined by the City Council in its annual budget deliberations.

The City operates on an annual Fiscal Year schedule beginning on July 1st and ending on June 30th.

Community Partnership Grants:

Community Partnership Grants are funds appropriated on an annual fiscal basis to community organizations that provide or enhance services that are generally considered within the purview of a governmental entity. If excess revenue is available, these organizations are pre-selected to receive funding during the City's annual budgetary process and will be included in the General Fund Budget. Community Partnership organizations include the following:

- The Charles Town Library;

DRAFT

- Jefferson County Community Ministries;
- Eastern Panhandle Transit Authority;
- Citizens Volunteer Fire Department; and
- Independent Fire Department.

In order to be eligible to receive funding in a subsequent budget cycle, Community Partnership Organizations must provide the Finance Director with an expenditure report, which is a statement detailing the expenditure of the City's allocation in the previous fiscal year. Expenditure reports are due on 31st of December each year, and failure to provide a report may result in loss of funding in future budgets.

Community Grants:

Community Grants are funding allocations provided to non-profit and civic organizations. Only nonprofit organizations shall be eligible to apply for a Community Grant. For purposes of this Policy, "nonprofit organization" means a business entity that is tax-exempt under sections 501(c)(3), (c)(4) or (c)(6) of the Internal Revenue Code of 1954, as amended. A person or group without nonprofit status may partner with a nonprofit organization to apply for a Community Promotion Grant. The details of the partnership should be clearly outlined and submitted with the application. Community Partnership Organizations are eligible to apply for Community Grants.

An eligible organization may apply for and receive up to two Community Grant awards within a single City fiscal year. Each application shall be evaluated separately under this Policy. Receipt of an award does not guarantee approval of a second award.

Application Process for Community Grants

Any nonprofit organization that desires financial assistance from the City must complete a Community Grant Application and attach a copy of its IRS determination letter and a copy of the most recent 990 tax return. If any of the aforementioned information is not available, please provide written explanation and attach to the Grant Application.

The application shall include a detailed description of the program and how it serves the residents of the City, how the grant funding will benefit the residents of the City, proof of good standing with the State of West Virginia and the City of Charles Town.

For an organization established within the two years preceding the date of its application, the City Council may, in its sole discretion, waive one or more application requirements, including required supporting documentation. The

DRAFT

organization shall identify the requirements for which a waiver is requested and explain why it cannot satisfy those requirements. Any waiver shall identify the requirements waived and any alternative information to be provided. A waiver of application requirements does not waive the eligibility requirements under this Policy, the prohibition on funding organizations that have previously misused City funds, the requirement to enter into a Letter of Agreement, or applicable reporting requirements.

The City reserves the right, in its sole discretion, to request additional information either in writing, in interviews or through scheduled presentations. Any organization not in good standing with the State of West Virginia will not be considered for financial assistance. An organization found to have misused City funds previously will not be eligible for grant funding.

Applications will be considered during the City's regular first revision of the fiscal year and during one additional application cycle within the fiscal year, at a time established by the City Council. Applications for the regular first-revision cycle will be due by May 31st of each year. The City Council shall establish and announce the submission deadline for the additional application cycle. An organization may receive no more than one Community Grant awards within a single City fiscal year.

In addition to evaluating the merits of each proposal as described in the application, the City Council will also consider the following factors:

- The projected number of City residents that will benefit from the program;
- Whether the organization appears to have the capacity to carry out the project, including necessary staff and financial resources;
- Other available funding sources and potential matches available for City funds;
- Whether the organization has been timely in completing reports for previous awards; and
- The success of previously funded programs.

The City Council will consider Community Grant Applications during the regular first revision of the fiscal year and the additional application cycle established by the City Council, and will award funds based upon the criteria outlined in this Policy.

Prior to distribution of any City funds, a Letter of Agreement shall be entered into between the City and the receiving organization. The Letter of Agreement will include a timeline, the amount of funding to be provided by the City, the work to be funded, required documentation to be provided by the organization, and any monitoring requirements. The Letter of Agreement shall also specify whether the grant will be paid on a cost-reimbursement basis or, for an award of less than

DRAFT

$5,000.00, in a lump sum, and shall identify the end date of the grant year and the expenditure-reporting requirement.

Reporting and Payment

Cost-Reimbursement Grants:
Except for grants approved for lump-sum payment as provided below, each Community Grant will be a cost-reimbursement grant in which the City will reimburse a grant recipient for expenditures once they have been incurred. To receive reimbursement, a grant recipient must submit invoices related to the grant work to the Finance Department for review. Once approved, grant funds will be released to the grant recipient.

Lump-Sum Grants Under $5,000.00:
The City Council may approve payment of a Community Grant award of less than $5,000.00 in a single lump sum rather than on a cost-reimbursement basis. The lump sum may be disbursed after the City and the receiving organization have entered into the required Letter of Agreement. An award of exactly $5,000.00 or more shall remain subject to the cost-reimbursement requirements above.

An organization receiving a lump-sum grant must file an expenditure report with the Finance Department at the end of the grant year identified in the Letter of Agreement. The report shall state how the grant funds were spent, including an itemized description of expenditures and the amount of any funds remaining unspent. Lump-sum payment does not waive the organization's obligation to use grant funds for the work specified in the Letter of Agreement or to comply with its documentation and monitoring requirements.

Effective
Original policy effective date: March 3, 2025.

Effective date of these amendments:

DRAFT

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2045: Cloud Data Storage Discussion

This agenda item was Tabled at the October 5, 2026, council meeting

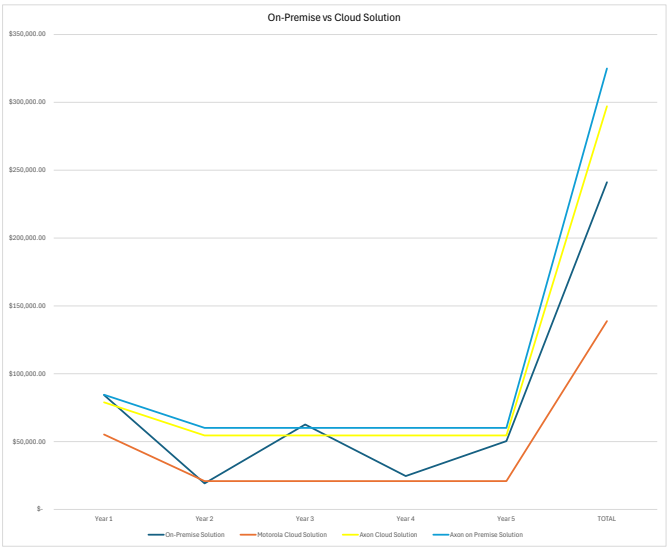
ATTACHMENTS:

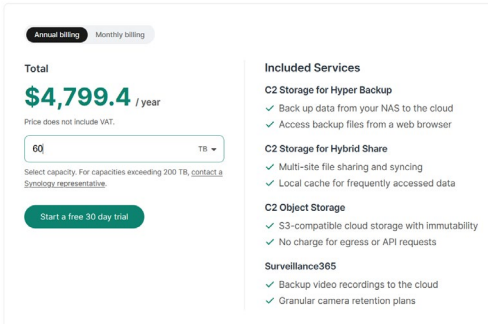
- Tek Advisors PremisevsCloud Summary.pdf
- Q_A Council Questions.pdf
- Motorola QUOTE - 3745884 - Charles Town - Cloud Migration 08212026.pdf
- Motorola QUOTE - 3805219 - Charles Town - (19) V700.pdf
- Motorola QUOTE - 3844710 - Charles Town - Deployment.pdf
- Axon Charles Town Police Department - WV_Q-917596.pdf
- Axon Charles Town Police Department - WV_Q-964558.pdf
- Axon Charles_Town_PD_Value_Brief_Q-917596-001.pdf
- Axon_print_productcards_onepagers_axonassistantonepager_8-5x11_03b-2.pdf
- Axon 2e0a6a4d-02c4-435f-8dba-559c01651219.pdf
- Axon 007.URCS_AxonFleet3.RespondProductCard_FNL.indd.pdf
- Axon Body 4 Product Card EN_US.pdf
- CaseGuard Charles Town Police Department 1 Ultimate Suite_V1.pdf
- CaseGuard_Studio_Hardware_Recommendations (1).pdf
- Estimate_1572_from_Executive_Emergency_Lighting_LLC.pdf
- CJIS_Security_Policy_v6-0_20241227 (1).pdf

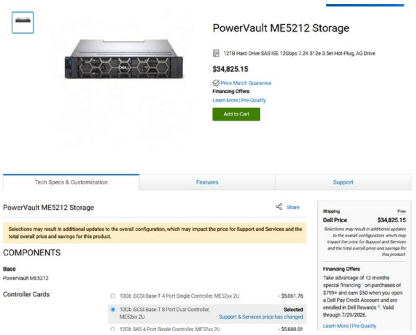
On-Premise Storage vs Cloud Solution

	Year 1	Year 2	Year 3	Year 4	Year 5		TOTAL
On-Premise Solution							
Compute Cost			$ 20,000.00				$ 20,000.00
Premise Storage Cost							
Tier 1 Storage	$ 34,825.15						$ 34,825.15
Tier 2 Storage	$ 18,877.07		$ 20,764.78		$22,841.25		$ 62,483.10
Backup Solution							
Tier 1 Backup	$ 1,200.00	$ 1,320.00	$ 1,452.00	$ 1,597.20	$ 1,756.92		$ 7,326.12
Tier 2 Backup	$ 4,799.40	$ 5,679.29	$ 6,959.13	$ 8,238.97	$ 9,518.81		$ 35,195.60
Motorola Storage Migration	$ 5,000.00						$ 5,000.00
CaseGuard Redaction Software	$ 4,548.00						$ 4,548.00
Redaction Software Computer	$ 4,000.00						$ 4,000.00
Current Motorla Subscription	$ 11,100.00	$ 12,210.00	$ 13,431.00	$ 14,774.10	$16,251.51		$ 67,766.61
TOTAL Solution Cost	$ 84,349.62	$ 19,209.29	$ 62,606.91	$ 24,610.27	$50,368.49		**$ 241,144.58**
Cloud Solution							
Motorola Cloud	$ 20,895.78	$ 20,895.78	$ 20,895.78	$ 20,895.78	$20,895.78		**$ 104,478.90**
Motorola Cameras	$ 34,325.94						**$ 34,325.94**
TOTAL Solution Cost	$ 55,221.72	$ 20,895.78	$ 20,895.78	$ 20,895.78	$20,895.78		**$ 138,804.84**
TOTAL Solution Difference						Savings	**$ (102,339.74)**
Redaction Labor							
Disaster Recovery Process							
Axon Cloud	$ 54,541.20	$ 54,541.20	$ 54,541.20	$ 54,541.20	$54,541.20		$ 272,706.00
Executive Lighting Old Equipment Removal	$ 24,412.40						$ 24,412.40
TOTAL Solution Cost	$ 78,953.60	$ 54,541.20	$ 54,541.20	$ 54,541.20	$54,541.20		**$ 297,118.40**
TOTAL Solution Difference						Increase	**$ 55,973.82**
Axon On Premise	$ 60,111.48	$ 60,111.48	$ 60,111.48	$ 60,111.48	$60,111.48		$ 300,557.40
Executive Lighting Old Equipment Removal	$ 24,412.40						$ 24,412.40
TOTAL Solution Cost	$ 84,523.88	$ 60,111.48	$ 60,111.48	$ 60,111.48	$60,111.48		**$ 324,969.80**
TOTAL Solution Difference						Increase	**$ 83,825.22**

	Year 1	Year 2	Year 3	Year 4	Year 5	TOTAL
On-Premise Solution	$ 84,349.62	$ 19,209.29	$ 62,606.91	$ 24,610.27	$50,368.49	$241,144.58
Motorola Cloud Solution	$ 55,221.72	$ 20,895.78	$ 20,895.78	$ 20,895.78	$20,895.78	$138,804.84
Axon Cloud Solution	$ 78,953.60	$ 54,541.20	$ 54,541.20	$ 54,541.20	$54,541.20	$297,118.40
Axon on Premise Solution	$ 84,523.88	$ 60,111.48	$ 60,111.48	$ 60,111.48	$60,111.48	$324,969.80







Storage used	**Storage**	**Needs Analysis**
Year 2022		
Year 2023	6TB	
Year 2024		
Year 2025		
Year 2026	55TB	
Year 2027		71TB
Year 2028		87TB
Year 2029		103TB
Year 2030		119TB

Comments:
Growth per year average 16.33TB

Questions posed by Councilman Hartman:

Motorola Response:

Default access scope — confirm current configuration is local/state-only, with federal or national sharing disabled unless we separately authorize it.

Charles Town PD is the sovereign owner of their CommandCentral DEMS instance. Inclusive of the data stored within that instance. Additionally, CCDEMS data is stored on Azure Government Cloud which is a dedicated isolated environment restricted to US Federal, state, and local government entities.

CommandCentral DEMS protects data with multiple security measures. To safeguard privacy and maintain strict CJIS compliance, the system encrypts all data in transit across public networks and at rest within the secure and isolated cloud. Federated single sign on (SSO) and customizable access permissions mean only approved users can access data.

Audit log standard — every external query logs a case number and legal basis. An agency name alone doesn't count.

CommandCentral DEMS delivers an unalterable, FIPS-compliant chain of custody by recording every view, download, redaction, and share in unalterable audit logs. Built to meet the highest evidence security mandates, the platform protects communications using AES-256 encryption at rest and TLS in transit, maintaining full compliance with the CJIS policy, the NIST 800-53 framework, and ISO 27001/27017/27018 standards.

Codified policy, not vendor default — Council adopts restrictions independent of whatever the vendor ships as default, so a software update can't quietly change our posture.

CommandCentral DEMS updates (specific to functionality) are released automatically, with a Release Notes notification sent directly to the administrator along with a pop up notification at login.

Charles Town PD would have control over deciding whether Firmware Updates for their V700 Body Worn Cameras happen automatically or are manually deployed to each camera.

Periodic review — someone at PD routinely pulls and reviews the logs on a site.

CommandCentral DEMS has a reporting subsection called CommandCentral Reporting which is available to provide detail reports tailored to the needs of the PD. Reports can be run, modified, or added at any time by administrative users.

City Attorney reviews the CJIA and Data sharing Addendums for the cloud storage and provides feedback to make sure those two documents are supporting city position.

Axon Response

Default access scope — confirm current configuration is local/state-only, with federal or national sharing disabled unless we separately authorize it.

Audit log standard — every external query logs a case number and legal basis. An agency name alone doesn't count.

Codified policy, not vendor default — Council adopts restrictions independent of whatever the vendor ships as default, so a software update can't quietly change our posture.

Periodic review — someone at PD routinely pulls and reviews the logs on a cite.

CJIA and Data sharing addendums for the cloud storage.

MOTOROLA SOLUTIONS







CHARLES TOWN, CITY OF

Cloud Migration

08/21/2026

The design, technical, pricing, and other information ("Information") furnished with this submission is confidential proprietary information of Motorola Solutions, Inc. or the Motorola Solutions entity providing this quote ("Motorola") and is submitted with the restriction that it is to be used for evaluation purposes only. To the fullest extent allowed by applicable law, the Information is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the Information without the express written permission of Motorola.
MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks a the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved.

08/21/2026

CHARLES TOWN, CITY OF
101 E WASHINGTON ST
CHARLES TOWN, WV 25414

RE: Motorola Quote for Cloud Migration

Dear Chris Kutcher,

Motorola Solutions is pleased to present CHARLES TOWN, CITY OF with this quote for quality communications equipment and services. The development of this quote provided us the opportunity to evaluate your requirements and propose a solution to best fulfill your communications needs.

This information is provided to assist you in your evaluation process. Our goal is to provide CHARLES TOWN, CITY OF with the best products and services available in the communications industry. Please direct any questions to Butch Bryant at butch.bryant@bearcom.com.

We thank you for the opportunity to provide you with premier communications and look forward to your review and feedback regarding this quote.

Sincerely,

Butch Bryant

Motorola Solutions Manufacturer's Representative

Billing Address:
CHARLES TOWN, CITY OF
101 E WASHINGTON ST
CHARLES TOWN, WV 25414
US

Quote Date:08/21/2026
Expiration Date:10/20/2026
Quote Created By:
Butch Bryant
butch.bryant@bearcom.com

End Customer:
CHARLES TOWN, CITY OF
Chris Kutcher
ckutcher@charlestownwv.us
3047252714

Contract: 36874 - SOURCEWELL MOBILE VIDEO-101223-MOT
AGREEMENT: WG AGREEMENT

Summary:

This Motorola quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the "Underlying Agreement") that authorizes Customer to purchase equipment and/or services or license software (collectively "Products"). If no Underlying Agreement exists between Motorola and Customer, then the following Motorola's Standard Terms of use and Purchase Terms and Conditions govern the purchase of the Products which is found at http://www.motorolasolutions.com/product-terms

Line #	Item Number	Description	Qty	Term	List Price
	V700				
1	WGP02950A	BATT LIION IP67 4050T	19		$123.75
2	WGB-0876A	V700 BWC 1080P FN READY W/REM BATT LM	19		$968.00
3	LSV07S03512A	ESSENTIAL SERVICE W/ACC DMG AND ADV REPLACEMENT - V700	19	5 YEARS	$552.00
	CommandCentral DEMS				
4	SSV00S03616A	SOFTWARE,COMMANDCENTRAL INTERVIEW ROOM SUBSCRIPTION*	1	5 YEAR	$0.00
5	PSV00S04239A	CC EVIDENCE VIRTUAL TRAINING*	1		$1,077.28
6	SSV00S05160A	COMMANDCENTRAL DEMS UNLIMITED STORAGE PER BODYWORN CAMERA*	19	5 YEAR	$1,020.00
7	SSV00S05161A	COMMANDCENTRAL DEMS UNLIMITED STORAGE PER IN-CAR VIDEO CAMERA*	48	5 YEAR	$1,020.00
8	SSV00S05158A	COMMANDCENTRAL DEMS PLUS SERVICE*	43	5 YEAR	$3,000.00

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Line #	Item Number	Description	Qty	Term	List Price
9	WGW00166-100	EL4 TO VIDEOMANAGER EL DATA MIGRATION SERVICE, PER TB OF DATA	35		$125.00
10	PSV00S05487A	MOBILE VIDEO REMOTE CLOUD DEPLOYMENT	1		$3,200.00
11	SSV00S06340A	RESPONDER PRODUCTIVTY ASSIST*	43	5 YEAR	Included
12	WGA00521-450	SERVER, UPLOAD, TOWER, 5 YEAR SUPPORT	1		$8,010.00

Subtotal $245,233.53

Total Discount Amount $106,428.69

Grand Total $138,804.84(USD)

Pricing Metric :

Price is indicative of the following -
# of Devices - 43

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Pricing Summary

		Payment Term	Upfront Sale Price
Upfront Costs*			
			$34,325.94
Upfront Subscription Fee			
	CommandCentral DEMS	Annually	$20,895.78
Sub Total:			**$55,221.72**

		Payment Term	Sale Price	Annual Sale Price
Year 2 Subscription Fee				
	CommandCentral DEMS	Annually	$20,895.78	$20,895.78
Year 3 Subscription Fee				
	CommandCentral DEMS	Annually	$20,895.78	$20,895.78
Year 4 Subscription Fee				
	CommandCentral DEMS	Annually	$20,895.78	$20,895.78
Year 5 Subscription Fee				
	CommandCentral DEMS	Annually	$20,895.78	$20,895.78
Sub Total:				**$83,583.12**

Grand Total System Price (Inclusive of Upfront and Annual Costs)	**$138,804.84**

**Upfront costs include the cost of Hardware, Accessories and Implementation, where applicable.*

Notes:

- The Pricing Summary is a breakdown of costs and does not reflect the frequency at which you will be invoiced.
- Additional information is required for one or more items on the quote for an order.
- Unless otherwise noted, this quote excludes sales tax or other applicable taxes (such as Goods and Services Tax, sales tax, Value Added Tax and other taxes of a similar nature). Any tax the customer is subject to will be added to invoices.
- Unless otherwise noted in this quote / order, installation of equipment is not included.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Line #	Item Number	Parametric Data
11	SSV00S06340A	Incomplete
4	SSV00S03616A	Incomplete
5	PSV00S04239A	Incomplete
6	SSV00S05160A	Incomplete
7	SSV00S05161A	Incomplete
8	SSV00S05158A	Incomplete

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

V700 BODY-WORN CAMERA SOLUTION DESCRIPTION

The V700 body-worn camera captures clear video and audio of every encounter from the user's perspective. Its continuous-operation capabilities allow constant recording, helping the user to capture every detail of each situation and create a reliable library of evidence for case building and review. The V700 can stream live video and report real time GPS location through a built-in LTE modem, directly to the suite of CommandCentral applications.

The V700 is easy to operate, with four control buttons. Its innate Record-After-the-Fact® (RATF) technology enables the device to capture important video evidence that can be retrieved hours or days after an incident occurs, even if a recording is not triggered by the user or sensor. With RATF, officers can prioritize response to immediate threats versus manually activating their camera.

KEY FEATURES OF THE V700

- **Detachable Battery –** The V700's detachable battery allows officers to switch to a fully-charged battery if their shift goes longer than expected. Since the battery charges without being attached to the V700, the battery is kept fully charged in the dock ready for use. This feature is especially helpful for agencies that share body-worn cameras with multiple officers.
- **Wireless Uploading –** Recordings made by the V700 are uploaded to the agency's evidence management system via LTE or WiFi. This enables easy transfer of critical recordings to headquarters for immediate review or long-term storage.
- **Real-time Location and Video Streaming –** With built-in LTE connectivity, the V700 paired with CommandCentral Aware will send location updates and stream live video to a dispatch center or Real Time Crime Center (RTCC) giving the agency a complete and accurate view of their officers for better coordination and quicker response times.
- **LTE Service Ready –** The V700 is approved for use on Verizon and FirstNet networks in the U.S. and Bell Mobility in Canada. The V700 will ship with a pre-installed SIM from both carriers, ready for service activation upon arrival with a data plan that best suits the agency's needs. LTE service activation would be on the agency's carrier account.
- **Data Encryption –** The V700 uses FIPS-140-2 compliant encryption at-rest and in-transit. This ensures recordings made by the agency's officers are secure from unauthorized access.
- **Record-After-The-Fact® –** Our patented Record-After-the-Fact® technology captures footage even when the recording function is not engaged. The camera user or admin can request video footage from a specific point in the past to be uploaded to the evidence management system, hours or even days after the event occurred.
- **Natural Field of View –** The V700 eliminates the fisheye effect from wide-angle lenses that warps video footage. Distortion correction ensures a clear and complete evidence review process. The V700's high quality, low light sensor captures an accurate depiction of recorded events, even in challenging lighting conditions.
- **SmartControl Application –** To maximize efficiency in the field, the Motorola Solutions SmartControl app enables V700 users to preview video recordings, add or edit tags, change camera settings and view live video from the camera. The app is available for both iOS and Android phones.
- **In-Field Tagging –** The V700 enables easy in-field event tagging. It allows officers to view event tags and save them to the appropriate category directly from the body-worn camera or via the SmartControl app.
- **Auto Activation –** The V700 body-worn camera(s) paired with an M500 or 4RE in-car video system(s) can form a recording group, which automatically starts recording when one of the devices begins to record. Each device can be configured to initiate a group recording using triggers like lights, sirens, doors, gun racks, and other auxiliary inputs. Up to eight V700s can form a recording group and collaborate on recordings, without a

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

corresponding in-car video system, using similar triggers. Group recordings are uploaded and automatically linked to the evidence management system as part of one event.

V700 AND IN-CAR VIDEO INTEGRATION

The V700 integrates seamlessly with the M500 or 4RE in-car video systems, capturing video of an incident from multiple vantage points. This integration includes the following features:

- **Distributed Multi-Peer Recording –** Multiple V700 body-worn cameras and in-car video systems can form a recording group and based on the configuration, automatically start recording when one of the devices begins to record. Group recordings are uploaded and automatically linked to the evidence management system as part of one incident.
- **Automatic Tag Pairing –** Recordings captured by integrated V700 body-worn cameras and in-car video systems can be uploaded to the evidence management system with the same tags. From the in-car video system's display, videos can be saved under the appropriate tag category. The tag is then automatically shared with the V700 video and uploaded as part of one incident along with the officer's name.
- **Evidence Management Software –** When V700 body-worn cameras and in-car video systems record the same incident, the Motorola Solutions evidence management software automatically links those recordings based on officer name, date, and time overlap.
- **Additional Audio Source –** The V700 can serve as an additional audio source when integrated with the in-car video system. The V700 also provides an additional view of the incident and inherits the event properties of the in-car video system's record, such as officer name, event category, and more, based on configuration.
- V700 and APX Radio Integration

Motorola Solutions' APX two-way radios can pair with V700 body-worn cameras to automate video capture through Bluetooth. When the APX's emergency mode button is pressed, or the Man Down feature is activated, the V700 is triggered to start recording immediately. The recording will continue until manually stopped by the officer via the start/stop button on the V700 or group in-car video system.

HOLSTER AWARE™ INTEGRATION

The V700 integrates with a Holster AwareTM sensor through Bluetooth. If configured, the sensor automatically prompts the V700 to record the moment the holstered equipment is drawn. The holster sensor information is stored with the V700 user profile and uploaded to the evidence management system. If the user is assigned to a different camera, the holster sensor information will be applied to the new camera. The holster sensor allows officers to record high-stress events as they unfold, without having to sacrifice situational awareness by manually activating the V700.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

DOCKING STATIONS

The V700 has three docking options:



Transfer Station – The Transfer Station is built for large, multi-location agencies with large numbers of V700 cameras in service at any given time. It can charge up to eight fully assembled body-worn cameras or individual batteries. The eight docking slots include an LED indication of a battery charging and upload status. While the V700 charges, the Transfer Station can automatically offload recordings from the camera to the evidence management system via an integrated 2.5Gb switch. The Transfer Station connects directly to the LAN for fast offload of recorded events to storage, while charging the body-worn camera battery. The Transfer Station supports comprehensive device management capabilities, such as camera configuration, checkout and officer assignment options; rapid checkout, kiosk, and individual camera checkout; automatic firmware and configuration updates.



USB Base – The USB Base charges the battery of a single V700 or standalone battery pack. The USB Base can be mounted in a vehicle or attached to a desktop or Mobile Data Computer with 12V or USB connection for power. The USB Base has LED indications for battery charging status and upload, and an ambient light sensor for optimal LED brightness control from bright sunlight to the dim interior of a patrol car. When connected to a laptop or desktop computer, the USB Base can be used to upload recordings to the evidence management system, as well as, receive firmware and configuration updates.



Wi-Fi Base – The Wi-Fi Base is mounted in a vehicle. It facilitates V700 upload of video evidence to the evidence management system, firmware updates, communication between V700 and in-car video system group devices and charges fully assembled V700s or individual battery packs. It has LED indications of battery charging status and upload, and an ambient light sensor for optimal LED brightness control, from bright sunlight to the dim interior of a patrol car.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

MOUNTING SOLUTIONS

V700 is compatible with the entire line of V300 mounting solutions as depicted below.

WGP02798	WGA00669	WGA00668	WGP02697	WGP03088	WGP03085
					
Magnetic Center Shirt Mount	Tek-Lok Belt Mount	Molle Locking Mount	Shirt Clip	Heavy Jacket Clip	Heavy Jacket Magnetic Mount

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

STATEMENT OF WORK — ESSENTIAL SERVICE FOR V700 BODY WORN CAMERA DEVICE (NORTH AMERICA)

This Statement of Work ("SOW") is subject to the terms and conditions of the Motorola Solutions Service Agreement or other applicable agreement in effect between the parties ("Agreement"). The terms of this SOW are an integral part of an Agreement with the Customer to which this SOW is appended and is made a part thereof by this reference. In the event of a conflict between the terms and conditions of an Agreement and the terms and conditions of this SOW, this SOW will control the inconsistency only. This SOW applies to the Device(s) specifically named in the Agreement.

DESCRIPTION OF SERVICES AND OBLIGATIONS

The term "Customer" refers to any end-user who has a purchase agreement with Motorola Solutions.

Essential Service provides either three (3) or five (5) years of coverage, as selected by the Customer, and includes:

- Remote Technical Support
- Software Maintenance
- Software Enhancements
- Hardware Repair for manufacturing defects

Motorola Solutions includes three (3) years of Essential Service with each Body Worn Camera (BWC) device purchase, with optional service upgrades to extend and/or provide additional coverage for the device.

ESSENTIAL SERVICE

Remote Technical Support

Remote Technical Support is provided for device issues related to software and/or hardware that require troubleshooting expertise. Motorola Solutions' System Support Center (SSC) and Technical Support Operations (TSO) center are staffed with highly trained technologists who specialize in the diagnosis and resolution of product issues. Motorola Solutions' SSC and TSO are continuously monitored against stringent, industry recognized incident and problem management processes.

Motorola Solutions will respond to calls, e-mails, and web portal submissions during normal support hours, five (5) business days per week, excluding holidays, and weekends. In addition, Customers may contact the Motorola Service Desk and a Motorola Solutions representative will log a technical request on Motorola Solutions' Case Management System.

Technical Problem Isolation, Analysis and Resolution.

A Motorola Solutions representative or technologists will:

- Work to isolate the problem/issue
- Analyze and determine the cause of the problem/issue
- Work to achieve problem/issue resolution

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Software Maintenance

Software maintenance is important for ensuring device performance and operation. Essential Service provides the Customer with access to the latest available Body Worn Camera (BWC) device operating system (OS) software, device firmware, and application software. Device software releases maintain the device software performance such that the Device operates in accordance with its specifications and documented functionality, and is aligned with the applicable Motorola Solutions infrastructure platform lifecycle. Each release may include bug fixes, security patches, and/or new feature activation enablements.

Configuration of the Body Worn Camera (BWC) device is made possible through the use of the CommandCentral DEMS, VideoManager EL On-Premises, or VideoManager EL Cloud, solution.

Access to software updates will remain available until the expiration of the initial term of the Essential Service Package. Upon expiration of the initial Essential Service term, availability of software updates will terminate, unless the Customer renews Essential Service.

Software Enhancements

Software Enhancements are included with all BWC devices that have a valid Essential Service Package. Software Enhancements may include, or introduce, new device features, functionality, or capabilities, that were not available at time of device purchase. Availability of software enhancements depends on the device hardware and software capability to work with the new enhancements. Certain enhancements, not included with Essential Service Packages, may only be available as an additional purchase.

Motorola Solutions, at its discretion, reserves the right to add new software enhancements, or remove existing software enhancements, from any of its Essential Service Package. Please contact your Motorola Solutions Sales associate, or visit the Motorola Solutions' Web portal, for additional information regarding device features and capabilities.

Software Enhancements for the device will be continuously available until the expiration of the initial term of the Essential Service Package. Upon expiration of the initial term of Essential Service, availability of Software Enhancements will terminate, unless the Customer renews Essential Service.

Device Hardware Repair

Essential Service provides the Customer with repair services at a Motorola Solutions owned and operated, supervised, or certified Repair Center that employs the latest test equipment and original or certified replacement components used in the manufacturing of the BWC device. Device Hardware Repair provides the Customer with repair services for internal and external device components that are damaged as a result of manufacturing defects and defects due to normal wear and tear. With this Service, the device is repaired to ensure full compliance with its specifications, as published by Motorola Solutions at the time of delivery of the original device via:

- Repairs, adjustments and restorations, if appropriate, of any device that malfunctions while being used within the operational and environmental parameters specified by Motorola Solutions.
- Device updates, if applicable, as may be released, from time to time, by Motorola Solutions in accordance with an Engineering Change Notice.

At the discretion of Motorola Solutions, if the device is considered “un-repairable”, for technical or economic reasons, Motorola will replace the device with a new or refurbished device.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

A three (3) year optional Service is available for the Transfer Station. Scope includes Technical Support and Hardware Repair as described in sections 1.2.1 and 1.2.4.

Essential Software Service

If for any reason the Customer declines or chooses to exclude the hardware repair option that is included with the three (3) year Essential Service Package, the Customer will automatically default to, and be entitled to, three (3) years of Essential Software Service and one (1) year of hardware repair against manufacturing defects, as covered by the standard product warranty.

Essential Software Service provides three (3) years of coverage and includes:

- Remote Technical Support
- Software Maintenance
- Software Enhancements

Scope of Products or Services included

Essential Service, and optional Service upgrades, are currently available for all V700 Body Worn Camera devices. Check with your Motorola Solutions' Sales representative if you have a question about the eligibility of your device.

Optional and purchasable Services are available for the Transfer Station.

MOTOROLA SOLUTIONS RESPONSIBILITIES

Software Release Availability. Motorola Solutions will provide access to the latest BWC device software and firmware releases via the CommandCentral DEMS, VideoManager EL On-Premises, or VideoManager EL Cloud, solution. For customers using the CommandCentral DEMS or VideoManager EL Cloud, software and firmware upgrades will occur automatically when the Body Worn Camera device connects to the agency's CommandCentral DEMS or VideoManager EL Cloud instance. If using the VideoManger EL On-Premises solution, the on-prem server will periodically connect to the VideoManager EL Cloud database to check for new software and firmware versions, download the latest version, and apply the new software and/or firmware automatically to the BWC device when it connects to the server.

Software Release Notes. Motorola Solutions may, from time to time, provide release notes for the BWC Device software release. Information regarding training material will be posted on the Learning Experience Portal (LXP) at https://learning.motorolasolutions.com

Hardware Repair. Motorola Solutions will provide repair or replacement of a device, at its option, with a five (5) business day in-house turnaround time, provided the device is delivered to the repair center by 9:00 a.m. (local repair center time), and replacement parts, components, and/or devices are available. Business days do not include holidays or weekends. Repair may include the replacement of parts, or boards with new parts or complete boards or, at Motorola Solutions' option, with functionally equivalent, reconditioned parts, boards, or with a new or refurbished replacement device. All replaced parts, boards or devices will become the property of Motorola Solutions. Turnaround time represents the time a product spends in the repair process; it does not include time in transit, including customs clearance.

LTE/4G Service. Motorola Solutions supports the operation of the V700 BWC device on multiple approved LTE/4G Carrier Networks. Based on the Customer's selection of a Carrier during the initial ordering process,

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Motorola Solutions will install, in the device, the Customer's selected Carrier SIM, before the device is shipped to the Customer. The Customer is responsible for contacting the Carrier and activating the LTE/4G data service.

Shipping. For devices repaired under Essential Service, Motorola Solutions will provide one-way shipping, from an Authorized Motorola Repair Center to the Customer. The Customer is responsible for the shipping method and any shipping costs incurred when returning the faulty device to an Authorized Motorola Solutions repair center. Based on the country of purchase, Motorola Solutions may also cover, or include, two-way shipping for the damaged or defective device. Eligibility for two-way shipping will be confirmed during the repair submission process.

CUSTOMER RESPONSIBILITIES

Serial Numbers. If device orders are submitted via Motorola Solutions' Partner Hub, OCC, or CPQ ordering systems, the hardware serial number(s) for three (3) year Essential Service and Essential Software, as well as five (5) year Essential Service, and three (3) and five (5) year Essential Service with Accidental Damage and Advanced Replacement, will be automatically captured and included in the Service Agreement.

If five (5) year Essential Service or three (3) and five (5) year Essential Service with Accidental Damage and Advanced Replacement is purchased within 90 days of device shipment, the Customer must provide a complete list, preferably in electronic format, or by completing a Service Order Form (SOF), of all hardware serial numbers to be covered under the Agreement.

Initiating Repair. When initiating a repair, the Customer must contact Motorola Solutions to obtain a Return Material Authorization (RMA) number for each faulty BWC device. The Customer can submit a repair, and request an RMA, via the Partner Hub Portal, or by contacting the Motorola Solutions' Service Desk. If two-way shipping is included, the customer can generate a shipping label via Partner Hub, or by contacting the Motorola Solutions Service Desk. The Return Material Authorization (RMA) must be included with the device when shipped to the Authorized Motorola Repair Center.

- Only the BWC device should be returned for repair. The battery must be removed before shipping the device to a Motorola Solutions Repair Center.
- Device accessories should not be included when returning a device to a Motorola Solutions Repair Center for repair. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.
- The SIM card must remain in the device, and intact, when the device is shipped to a Motorola Solutions Repair Center. If the SIM card is removed, or if any evidence of SIM card tampering is found, including disassembling of the device, the warranty will be null and void.

Motorola Solutions is not responsible for any accessories, or device batteries, that are shipped with the device for repair.

Device software releases. The Customer will be responsible for updating each eligible BWC device with the latest available software and/or firmware, and of advising users of any operational changes that may have been introduced as a result of the new software or firmware.

LTE/4G Service. The Customer is responsible for selecting a Motorola Solutions approved LTE/4G Carrier/Provider during the initial ordering process, and for contacting the Carrier and activating LTE service for the device. The Customer is solely responsible for all financial obligations with the selected LTE Carrier.

Wi-Fi Connectivity. The Customer is responsible for providing all Wi-Fi connectivity to the device.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Removing Customer Data. The Customer is responsible for removing, from the device, any data, video, or other information that the Customer wishes to retain or destroy, prior to sending the device to a Motorola Solutions Repair Center for repair.

Motorola Solutions may provide a Video Evidence Recovery Service for the BWC device, as an additional charge. Video Evidence Recovery is a best effort service that is dependent on the condition of the device. This service, if applicable, will have a separated Agreement, with Terms and Conditions, outside the scope of this Statement of Work (SOW). Please contact your Motorola Solutions Representative for more information regarding the Video Evidence Recovery Service.

ESSENTIAL SERVICE LIMITATIONS AND RESTRICTIONS

Customer will incur additional charges at the prevailing rates for any of the following activities, which are not covered under this Agreement:

- Replacement of consumable parts or accessories, as defined by product, including but not limited to batteries, cables, mounts, or clips.
- Repair of problems caused by natural or manmade disasters, including but not limited to fire, theft and floods that would cause internal or external component damage or destruction.
- Repair of problems caused by third parties' Software, accessories or peripherals not approved in writing by Motorola Solutions for use with the device.
- Repair of problems caused by using the device outside of the product's operational and environmental specifications, including improper handling, carelessness or reckless use, or repaired by a third party.
- Repair of problems caused by unauthorized alterations or attempted repair.
- Non-remedial work, including but not limited to administration and operator procedures, reprogramming, and operator or user training.
- Problem determination and/or work performed to repair or resolve issues with non-covered products; for example, any hardware or software products not specifically listed on the service order form.
- Any file or video backup or restoration.
- Completion and test of incomplete application programming or system integration if not performed by Motorola Solutions and specifically listed as covered.
- Use of Software or Firmware releases, except as provided for under the responsibilities outlined in this document.
- Accidental damage, chemical or liquid damage, or other damage caused outside of normal device operating specifications, unless the Customer has purchased the optional Essential Service with Accidental Damage and Advanced Replacement package.
- Cosmetic imperfections that do not affect the functionality of the device.

Where a Body Worn Camera device is submitted for repair that is outside the scope of Service, such repair may be quoted by Motorola Solutions for additional cost in accordance with Motorola Solutions' standard Time and Materials (T&M) rates and terms and conditions. Motorola Solutions will notify the Customer of any incremental charges related to the aforementioned exclusions prior to completing the repair and said repair will be subject to acceptance of the quotation by the Customer.

Software support for unauthorized modifications, or other misuse of the device software, is not covered under this Agreement.

Access to the software and firmware releases for updating the device under this SOW is available only for the device named in the Agreement. Software updates to any additional devices are expressly excluded and

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

prohibited. Notwithstanding the foregoing, Motorola Solutions may, at its sole discretion, include coverage for other devices.

Any implementation tools not required to support the device software and firmware updates are excluded from coverage.

MOTOROLA SOLUTIONS IS NOT OBLIGATED TO PROVIDE SUPPORT FOR ANY DEVICE:

- That has been repaired, tampered with, altered or modified (including the unauthorized installation of any software) — except by Motorola Solutions authorized service personnel.
- That has been subjected to unusual physical or electrical stress, abuse, or forces or exposure beyond normal use within the specified operational and environmental parameters set forth in the applicable product specification.
- If Customer fails to comply with the obligations contained in the product purchase agreement and/or the applicable software license agreement and/or Motorola Solutions terms and conditions of service.

ESSENTIAL SERVICE WITH ACCIDENTAL DAMAGE REPAIR AND ADVANCED REPLACEMENT

Description of Services and Obligations

Accidental Damage coverage is an optional, prepaid service that adds coverage for accidentally damaged BWC devices. Accidental Damage coverage must be purchased together with, or within 90 days of, a qualifying Motorola Solutions device purchase. This three (3) or five (5) year service offer reduces unexpected expenses related to the repair of the device. Accidental Damage and Advanced Replacement coverage includes all services provided under Essential Service, plus additional coverage for Accidental Damage and Advanced Replacement of the damaged device.

Examples of repairs covered under Accidental Damage include:

- Electrical repair for failures caused by accidental water or chemical damage
- Electrical repair for accidental internal damage
- Replacement of accidentally cracked or broken housings.
- Replacement of accidentally cracked or broken camera lens or displays.
- Replacement of accidentally cracked or broken or missing buttons, knobs, or keypads

Repair or Replacement. Motorola Solutions will provide repair or replacement of a BWC device, at its option, with a five (5) business day in-house turnaround time, excluding weekends and holidays, provided the device is delivered to the repair center by 9:00 a.m. (local repair center time), and replacement parts, components, and/or devices are available. Repair may include the replacement of parts, or boards with new parts or complete boards or, at Motorola Solutions option, with functionally equivalent, reconditioned parts, boards, or with a new replacement or refurbished device. All replaced parts, boards or devices will become the property of Motorola Solutions. Turnaround time represents the time a product spends in the repair process; it does not include time in transit, including customs clearance.

Serial Numbers. If the Accidental Damage Service is purchased with the device, in the same order, using Motorola Solutions' Partner Hub Portal, OCc, or CPQ when ordering, the hardware serial number(s) are automatically captured and included in the Service Agreement. If Accidental Damage Service is purchased within 90 days of device shipment, the Customer must provide a complete list, preferably in electronic format, or by completing a Service Order Form (SOF), of all hardware serial numbers to be covered under the Agreement.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Initiating Repair. When initiating a repair, the Customer must contact Motorola Solutions to obtain a Return Material Authorization (RMA) number for each faulty BWC device. The Customer can submit a repair, and request an RMA, via the Partner Hub Portal, or by contacting the Motorola Solutions' Service Desk. If two-way shipping is included, the customer can generate a shipping label via Partner Hub, or by contacting the Motorola Solutions Service Desk. The Return Material Authorization (RMA) must be included with the device when shipped to the Authorized Motorola Repair Center.

- Only the BWC device should be returned for repair. The battery must be removed before shipping the device to a Motorola Solutions Repair Center.
- Device accessories should not be included when returning a device to a Motorola Solutions Repair Center for repair. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.
- The SIM card must remain in the device, and intact, when the device is shipped to a Motorola Solutions Repair Center. If the SIM card is removed, or if any evidence of SIM card tampering is found, including disassembling of the device, the warranty will be null and void.

Motorola Solutions is not responsible for any accessories, or device batteries, that are shipped with the device for repair.

Advanced Replacement. Under Accidental Damage and Advanced Replacement Service, Motorola Solutions will provide Advanced Replacement for the damaged device. Motorola Solutions will ship a new or refurbished replacement device to the Customer within two (2) business days of receiving the Customer repair request, subject to availability of replacement devices. Business days do not include weekends or holidays.

The Customer must return the defective or damaged device to a Motorola Solutions Repair Center within 30 days after receiving the replacement device. Failure to return the damaged device to Motorola Solutions will result in an additional Customer charge for the replacement device.

When returning a device for Advanced Replacement, device accessories should not be included. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.

Motorola Solutions is not responsible for any accessories that are shipped with the device.

ACCIDENTAL DAMAGE AND ADVANCED REPLACEMENT LIMITATIONS AND RESTRICTIONS

Customer will incur additional charges at the prevailing rates for any of the following activities, which are not covered under this Agreement:

- Replacement of consumable parts or accessories, as defined by product, including but not limited to batteries, chargers, charging stations, mounts, and clips.
- Repair of problems caused by natural or manmade disasters, including but not limited to fire, theft and floods that would cause internal or external component damage or destruction.
- Repair of problems caused by third parties' Software, accessories or peripherals not approved in writing by Motorola Solutions for use with the device.
- Repair of problems caused by using the device outside of the product's operational and environmental specifications, including improper handling, carelessness or reckless use, or repair by a third party.
- Repair of problems caused by unauthorized alterations or attempted repair.
- Non-remedial work, including but not limited to administration and operator procedures, reprogramming, and operator or user training.
- Problem determination and/or work performed to repair or resolve issues with non-covered products; for example, any hardware or software products not specifically listed on the service order form.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

- Any file or video backup or restoration.
- Completion and test of incomplete application programming or system integration if not performed by Motorola Solutions and specifically listed as covered.
- Use of Software or Firmware releases except as provided for under the responsibilities outlined in this document.

There is a maximum limit of one (1) Body Worn Camera device repair, per contract year, for Essential Service with Accidental Damage and Advanced Replacement.

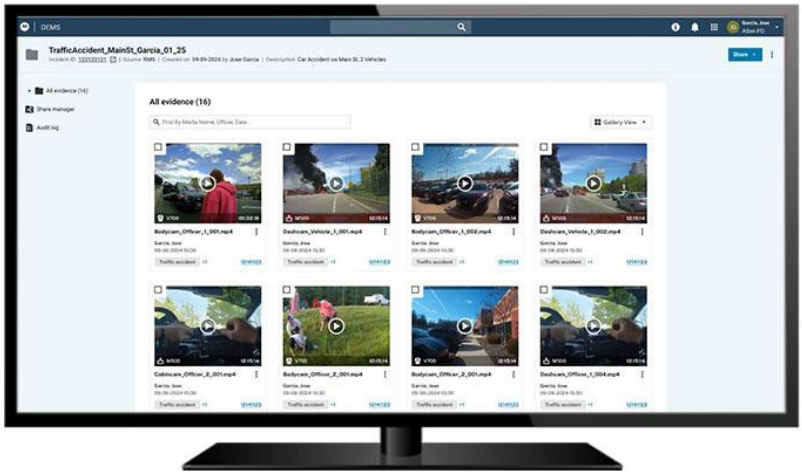
Where ongoing “Accidental Damage” repair is deemed by Motorola Solutions to be excessive, systemic, or the result of device mishandling, the Customer may be subject to an additional charge. Should the accidental damage continue unabated, the Customer will incur repair charges at Motorola Solutions’ discretion and prevailing charges for devices deemed by Motorola Solutions to have been damaged through improper handling, carelessness or reckless use.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

COMMANDCENTRAL DEMS PLUS SOLUTION DESCRIPTION

OVERVIEW

CommandCentral DEMS provides a suite of digital evidence management tools that help users contain, organize, and act on large amounts of incoming multimedia. These tools streamline the collection, capture, storage, and sharing of data from a single location.



By centralizing digital evidence collections, CommandCentral DEMS removes data silos and provides users with the storage and tools they need to get the most out of their critical information. In addition, users can easily secure and share content with an intact chain of custody, to improve collaboration.



CommandCentral DEMS Plus is available without any upfront capital investment. Monthly subscription service costs include the software, device management, and storage. Evidence also secures data at rest and in transit to protect communications. This complies with CJIS guidelines and the NIST framework.

THE COMMANDCENTRAL PLATFORM

CommandCentral is an end-to-end platform of interconnected solutions that unify data and streamline public safety workflows from a tip or call to case closure. Through single sign-on capabilities, your personnel can access all software applications with one agency username and password for a more streamlined workflow. The platform puts your agency's data to better use, improves safety for critical personnel, and helps keep your focus on the communities you serve.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

CommandCentral continuously evolves, maximizing the value of existing investments while adopting new capabilities that better meet your personnel's growing needs. With cloud-based services and an agile development methodology through constant user feedback, Motorola Solutions can deliver new features and functionality in a more manageable, non-intrusive way.



Figure 1: The End-to-End Platform

DIGITAL EVIDENCE MANAGEMENT

Evidence stored in the tool is easy to search, correlate, and review alongside other case-related information from your CAD or RMS database. Relevant content can be marked and intelligently sorted to quickly locate critical information from a central touchpoint. This unified storage framework allows personnel to make informed decisions from an organized and complete case evidence view, while offering an access control system to allow only authorized personnel to view sensitive information.

Store and Manage - Collections

Evidence is automatically linked based on the tags and metadata attached to those files, helping users find additional contextual information on an incident and build cases quickly. Users can search and filter content to locate additional relevant data to link to a case or incident.

- **Auto Created Collections** – Digital evidence captured by integrated products that provide a Record ID, such as an Incident or Case Number, will automatically be grouped into a Collection.
- **Manually Created Collections** – Users can manually create collections or sub-collections to better organize individual files and related items.
- **Bulk Actions** – Easily download, share, and edit specific details of multiple files in a group.
- **Manual Upload** - Upload digital evidence from 3rd parties directly into an existing collection or while creating a new collection to build your case.

Interagency, Judicial, and Community Sharing

Easily share digital evidence with trusted organizations and community members using our secure sharing features.

- **Trusted Organizations, Authenticated Sharing** - Share digital evidence collections with other agencies and judicial partners in a secure portal accessible by authenticated users.
- **Unauthenticated** - Quickly share evidence with the community for public information requests. Links can be password protected to add a level of security.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

AI Assisted Redactions and Transcriptions

Protect confidentiality and save time with our AI Assisted Redaction and Transcription Services.

- **AI Transcription & Summaries** - Generate transcriptions on-demand or set up automations to create transcriptions for video and audio files with an AI generated summary.
- **AI Assisted Video and Audio Redactions** - Receive suggestions for objects and information commonly redacted.
  - Video Object Detection - Identifies and tracks objects commonly redacted; such as heads (faces), license plates, screens, and documents.
  - Audio Detections - Use AI to auto-detect common sensitive data found in audio; such as names, phone numbers, and medical interactions.
  - Manual Redactions - For simple projects, manual redaction tools are available.

Current MSI Ecosystem Integrations:

- CommandCentral Responder Starter, Mobile Field Responder Application
- SmartControl Mobile App for Body Cameras
- 10-21 Police Phone
- CAPE-Equipped Drones
- Smart Transcription for 9-1-1 call recordings
- ViQi - Voice Activated AI
- Records Management
  - Flex Records
  - PremierOne Records
  - CC Records / RMS

Third Party Integrations

Import and export of data from some 3rd party software is available in some instances. Talk to your sales team for more details.

DEVICE MANAGEMENT

Easily manage, configure, deploy and monitor in-car and body cameras in CommandCentral DEMS.

- **Body Cameras** are checked out to a given officer with assignment records showing the history of use for the device.
- **In-Car Video** systems are configured with a list of officers who are authorized to use it. When an officer logs into the device, they are marked as the owner of any evidence created by the device.
- **Rapid Checkout Kiosk** allows users to quickly check out pooled body cameras at the beginning of a shift with an easy-to-use interface.
- **User Preferences -** In-car and Body cameras can be configured to remember preference settings for each user, including alert volume level, haptic notifications, screen and LED brightness and more.
- **Automatic Video Upload**: Videos are automatically uploaded to CommandCentral DEMS and linked based on officer name, or group recordings.
- **Device Dashboard:** See a detailed, easy-to-understand overview of your body cameras and in-car video systems at a glance, including their battery levels, memory levels, last checkout, and location.
- **In-field tagging:** Categorize and review body camera footage while still in the field, via the SmartControl iOS/Android/Windows app.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Supported devices include:

- SVX converged Radio Speaker Mic and Body-Worn Camera
- V700 Body Cameras
- M500 In-Car Camera System

CLOUD SECURITY AND COMPLIANCE

Proactive Security Design

Security is proactively incorporated into the design of our applications, not applied reactively when incidents occur. Applications undergo security reviews at each phase of their development and continue with ongoing assessments after deployment to find and repair vulnerabilities.

Compliance with Industry Best Practices

Our cloud solutions comply with key industry best practices for security, including NIST Security and Privacy Controls for Information Systems and Organizations (800-53), ISO 27001, 27017, 27018 - Specification for an Information Security Management System, and Criminal Justice Information System (CJIS) Security Policy. We conduct continuous and comprehensive risk assessments following the guidelines and best practices provided by NIST and ISO.

Cybersecurity Champions Imbedded in Product and Service Teams

Over 350 specially trained and certified Cybersecurity Champions ensure that a culture of cybersecurity is instilled into the fabric of our product and services teams. Programmers receive ongoing security training and updates on the latest hacker tactics so they can layer security into every stage of the application development process.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

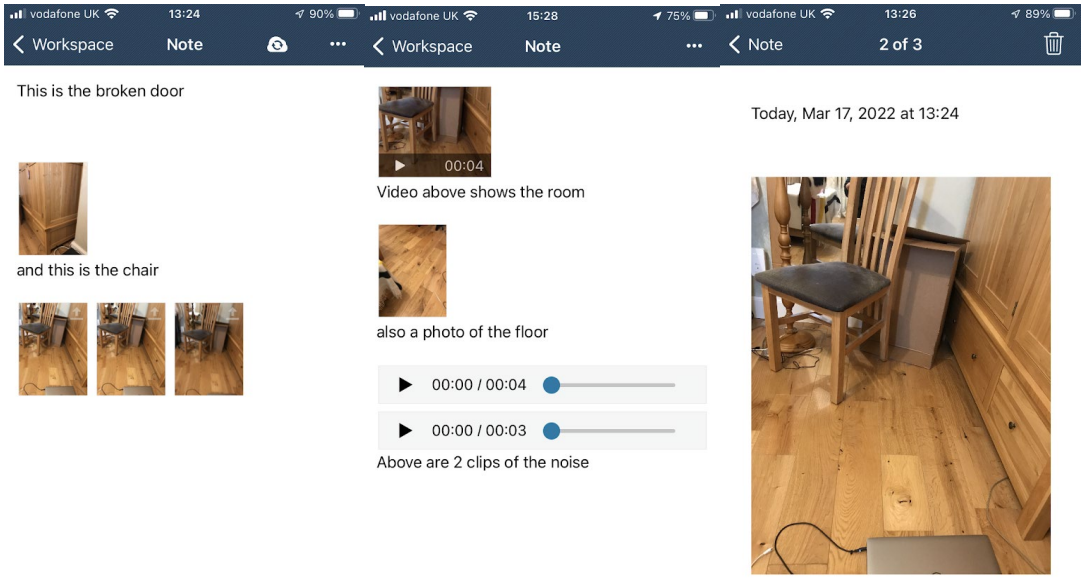
COMMANDCENTRAL RESPONDER STARTER WITH EVIDENCE SOLUTION DESCRIPTION

CommandCentral Responder is a mobile solution for frontline Responders. This includes an application for iOS and Android.

The Responder with Evidence solution (also known as Responder Starter) allows users to capture media, record notes, tag items and link them to cases / incident records. Depending on which feature flags are enabled, a customer can gain access to different sets of features. Using a note, users can capture a group of photos in one go and then tag them or link them all as a group. Responder uploads media automatically once captured, making the process easy for users. Media is removed automatically from a user's device after a customer defined retention period. Users can set up the application easily by downloading the application from App Store or Play Store, and simply logging in with their MSI account.

NOTES AND MEDIA CAPTURE

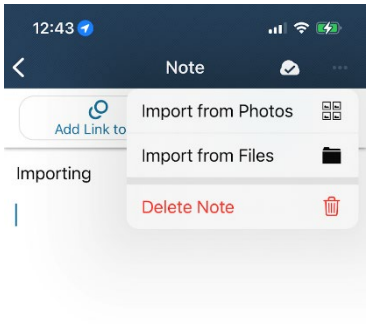
Responder with Evidence allows a user to create a note and capture media and associated text. Users can use the note either just to group a set of media together (as they capture it) or to add additional explanatory text as they capture details. Users can capture audio, video and photographs in this collection. This means users can attend a scene and immediately capture a collection of media before working out how to tag or link it. Users can view a full size version of a photo and can zoom in to view it at larger scale.



Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

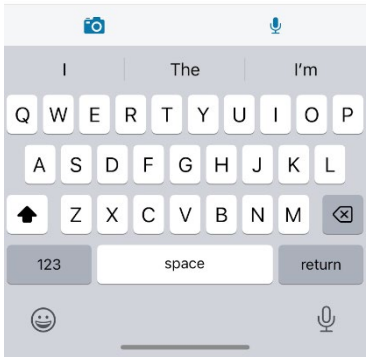
IMPORTING MEDIA

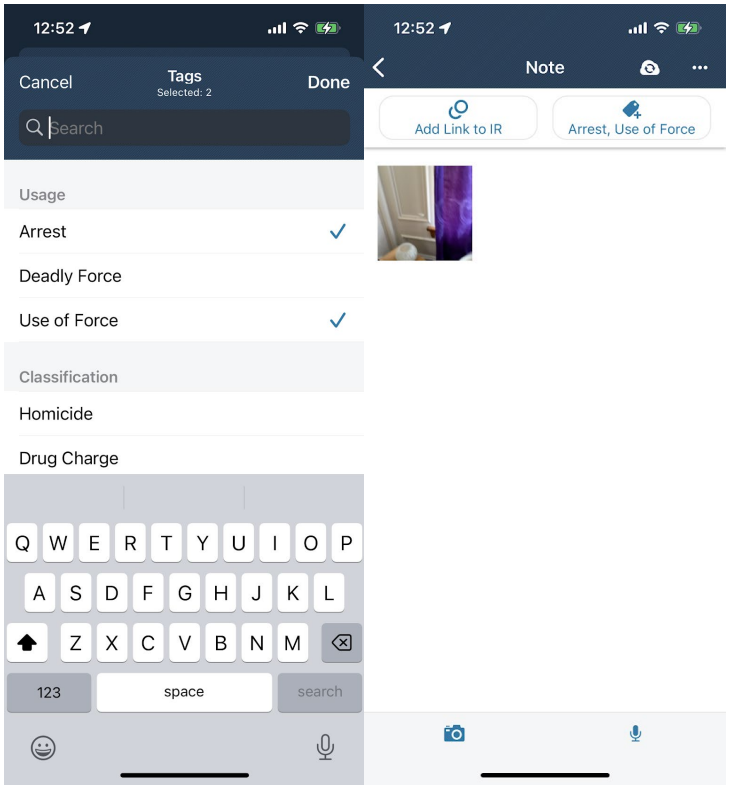
Users can import media (photos, audio, video and files such as PDFs) from their gallery or file system - allowing them to use media files shared to their device by members of the public. This feature can be enabled or disabled using per agency configuration (if an agency does not want to use this capability they can turn it off).



TAGGING

Users can choose to tag a note, which will tag it and all media within it. Tags provided are those configured by the agency and are shown grouped by categories defined by the agency. Selected tags will then show on the note. As with all media, in CommandCentral Evidence, tags are used to manage and set the retention period for media. In addition to manual tags, Responder can be configured to set a default “Responder Media” tag on every media item uploaded by Responder. This allows agencies to set a default tag & retention period for anything captured by Responder.





LINKING TO RECORDS

Users can link a note to an incident record contained in the CommandCentral Consolidated Records View - to relate the note & media to the incident and ensure they are shown in the Consolidated Records View.

The incident record summary shown in Responder contains key data for the record - Report number, Incident Type, Involved officers & Incident Start & End Date.

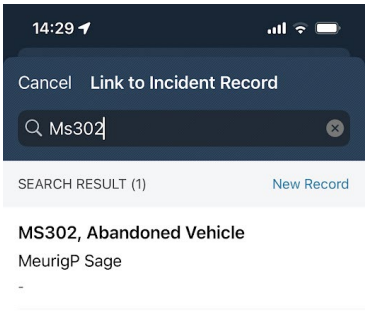
Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

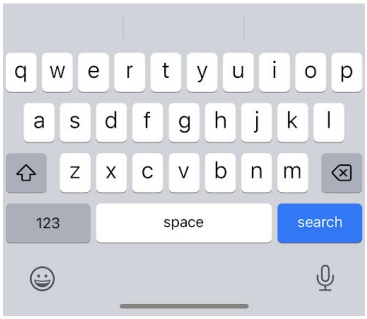
Users can:

- Link to an incident record already on a user's device
  - Any incident records for which a user is already added as an involved officer will be automatically downloaded to their device.
- Link to an incident record by search:
  - A user can search for an incident record using a simple free text search, searching for any incident record for the agency in CC Records that the user has permission to view
- Create a new incident record if one does not exist (not available with Flex - see below)
  - User can create a new incident record (providing summary details above).
  - User will be provided with the Report number separately
  - Responder application will detect creation of incidents (from Responder) with duplicate Report numbers, warn users and allow them to resolve conflicts.

The exact behavior depends on whether the customer is using:

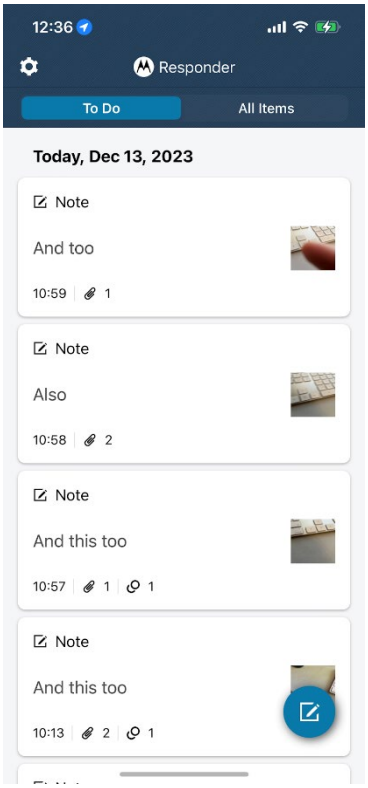
- Responder with CommandCentral Evidence connected to Flex
  - Flex generates law incidents (typically created from CAD). These law incidents are uploaded to CC Records and user can link to these. Whenever there is a case number to link to there will be a law incident in Flex and this will be pushed to CC Records. As a result, users can't create incident record summaries in Responder, they can link to law incidents created in Flex.
- Responder with CommandCentral Evidence connected to P1 RMS
  - P1 RMS manages case reports in case folders. If there is a case report, then P1 uploads this to CC Records and users can link to it.
  - If there is a case folder in P1 RMS but no case report then users can create an incident record summary in Responder, adding the case number - allowing the user to link media to the case.
- Responder with CommandCentral Evidence standalone (with CommandCentral Records Starter capability)
  - Users can create incident record summaries or link to ones that have already been created.
  - Incident records have to be manually created in Responder (or the CommandCentral Evidence/Records web UI) - they aren't imported from other systems





Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

TIMELINE



Users can view previous notes in their timeline:

- Update a note later with further information;
- Refer back to them later when completing a report;
- Notes (and associated media) are kept on the device in a user's timeline for an agency configured period - configured in CC Admin (default is 30 days).

The timeline is separated into a To Do and All Items view.

The To do view shows notes that a user has added, that are either less than 24 hours old or that have not yet been linked to an incident record. Users can manually move a note out of the To do view if they don't intend to link it to an incident record. However, typically users are encouraged to capture media and then link it. This provides an easy way for users to see notes they still have to deal with.

The All Items view shows all notes on a user's device so they can find older notes & evidence that they need to refer to.

SYNCHRONIZING DATA

Notes & media files are automatically uploaded to CommandCentral Evidence - a synch indicator is shown on the note to show data is being uploaded, and an indicator is shown on each media item to show that the media item is being uploaded.

When a user signs out of Responder app, if they have unsent data (notes & evidence) then Responder will alert the user that they have unsent items - allowing them to ensure they are in an area of coverage and wait for sync to complete.

AUTHENTICATION AND SECURITY

CommandCentral Responder prevents unauthorized users from accessing the data transmitted to and from mobile devices through an HTTPS connection with FIPS 140-2 Transport Layer Security (TLS) v1.2 encryption. All user requests and other user data are protected by Azure Government services.

To access the system, a user authenticates against the CommandCentral Identity Management system. If desired, the identity management system can be setup to federate authentication against a customer identity management system such as Azure AD.

Customers can enable multi-factor authentication.

- If a customer uses CommandCentral Identity Management directly then multi factor authentication can be enabled for any or all users (at customer decision). If enabled then users need to enter a username & password and a second factor which is either a one time passcode sent by email or a one time passcode or authentication approval enabled via a separate app (Ping ID).
- If a customer uses federated authentication then the federated auth system authenticates the user. In this case the customer identity management will implement the multi factor authentication. For instance, Azure AD can enforce multi factor authentication and allows a one time passcode to be provided via email, SMS or via the Azure authenticator app.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

In addition, Responder uses a PIN code (or optionally biometric unlock) that is used to allow users to unlock their app after inactivity timeout. Sign in online is required once per shift to access online data.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

MOTOROLA SOLUTIONS







CHARLES TOWN, CITY OF

Charles Town PD Body Worn Camera Quote

09/04/2026

The design, technical, pricing, and other information ("Information") furnished with this submission is confidential proprietary information of Motorola Solutions, Inc. or the Motorola Solutions entity providing this quote ("Motorola") and is submitted with the restriction that it is to be used for evaluation purposes only. To the fullest extent allowed by applicable law, the Information is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the Information without the express written permission of Motorola.
MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks a the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved.

09/04/2026

CHARLES TOWN, CITY OF
101 E WASHINGTON ST
CHARLES TOWN, WV 25414

RE: Motorola Quote for Charles Town PD Body Worn Camera Quote

Dear Chris Kutcher,

Motorola Solutions is pleased to present CHARLES TOWN, CITY OF with this quote for quality communications equipment and services. The development of this quote provided us the opportunity to evaluate your requirements and propose a solution to best fulfill your communications needs.

This information is provided to assist you in your evaluation process. Our goal is to provide CHARLES TOWN, CITY OF with the best products and services available in the communications industry. Please direct any questions to Butch Bryant at butch.bryant@bearcom.com.

We thank you for the opportunity to provide you with premier communications and look forward to your review and feedback regarding this quote.

Sincerely,

Butch Bryant

Motorola Solutions Manufacturer's Representative

Billing Address:
CHARLES TOWN, CITY OF
101 E WASHINGTON ST
CHARLES TOWN, WV 25414
US

Quote Date:09/04/2026
Expiration Date:11/03/2026
Quote Created By:
Butch Bryant
butch.bryant@bearcom.com

End Customer:
CHARLES TOWN, CITY OF
Chris Kutcher
ckutcher@charlestownwv.us
3047252714

Contract: 36874 - SOURCEWELL MOBILE VIDEO-101223-MOT
AGREEMENT: WG AGREEMENT

Line #	Item Number	Description	Qty	Term	List Price	Sale Price	Ext. Sale Price	Refresh Duration
	V700							
1	WGP02950A	BATT LIION IP67 4050T	19		$123.75	$99.00	$1,881.00	
2	WGB-0876A	V700 BWC 1080P FN READY W/REM BATT LM	19		$968.00	$774.40	$14,713.60	3 YEAR
3	LSV07S03512A	ESSENTIAL SERVICE W/ACC DMG AND ADV REPLACEMENT - V700	19	5 YEARS	$552.00	$441.60	$8,390.40	
4	PRODUCT_REFRESH	VIDEO EQUIPMENT,PRODUCT REFRESH	19		$800.00	$640.00	$12,160.00	
	VideoManager EL or EX: Video Evidence Management							
5	WGP02400-500	LICENSE,VIDEOMANAGER EL ON-PREM SITE LICENSE KEY	1		$1,250.00	$1,000.00	$1,000.00	
6	WGP02400-520	VIDEOMANAGER EL, BODY WORN CAMERA ANNUAL LICENSE	19	1 YEAR	$243.72	$194.98	$3,704.62	

Grand Total $41,849.62(USD)

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Pricing Summary

	Payment Term	Upfront Sale Price
Upfront Costs*		
		$38,145.00
Upfront Subscription Fee		
VideoManager EL or EX: Video Evidence Management	Annually	$3,704.62
Sub Total:		**$41,849.62**

	Payment Term	Sale Price	Annual Sale Price
Sub Total:			**$0.00**

Grand Total System Price (Inclusive of Upfront and Annual Costs)	**$41,849.62**

**Upfront costs include the cost of Hardware, Accessories and Implementation, where applicable.*

Notes:

- The Pricing Summary is a breakdown of costs and does not reflect the frequency at which you will be invoiced.
- Unless otherwise noted, this quote excludes sales tax or other applicable taxes (such as Goods and Services Tax, sales tax, Value Added Tax and other taxes of a similar nature). Any tax the customer is subject to will be added to invoices.
- Unless otherwise noted in this quote / order, installation of equipment is not included.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Line #	Item Number	Parametric Data
6	WGP02400-520	ADMEMAIL = ckutcher@charlestownwv.us,ADMUSER = Chris Kutcher

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

VIDEOMANAGER EL SOLUTION DESCRIPTION

VideoManager EL simplifies evidence management, automates data maintenance and facilitates management of your department's devices.



It is compatible with V300 and VISTA body-worn cameras, as well as M500 and 4RE in-car video systems, enabling you to upload video evidence quickly and securely.

The optional SmartControl and SmartConnect smart device applications support live video streaming from body-worn cameras, allowing personnel to view footage captured by the cameras in the app.

VIDEO EVIDENCE MANAGEMENT

VideoManager EL delivers benefits to all aspects of video evidence management. From streamlining the evidence review process to automatically maintaining your stored data, VideoManager EL makes evidence management as efficient as possible. With VideoManager EL, you minimize the amount of time spent manually managing evidence, allowing your team to spend more time in the field.

Simplified Evidence Review

VideoManager EL makes evidence review easier by allowing you to upload captured video and audio from your in-field devices, sharing important information that groups relevant evidence together. This information includes a recording's date and time, device used to capture, event ID, officer name and event type. Incidents recorded from several devices can be found easily and viewed at the same time, eliminating the task of reviewing irrelevant footage.

Its built-in media player includes a visual display of incident data, allowing you to view moments of interest, such as when lights, sirens or brakes were activated during the event timeline, status of cameras and microphones and patrol speed graph.

Other relevant files, such as PDFs, spreadsheets, reports, third-party videos, audio recordings, pictures, drawings and applicable external files can also be grouped together and stored under a specific case entry, allowing all pertinent information to be stored together in Evidence Library.

Easy Evidence Sharing

VideoManager EL empowers you to easily share information in the evidence review or judiciary sharing process by exporting evidence data. It is capable of searching for data using various criteria, including import, export, playback, download, share and modification dates, allowing users to quickly find relevant evidence.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Automatic Data Maintenance

VideoManager EL lets you automatically organize the evidence data you store, allowing you to save time that would be spent manually managing it. It can schedule the automatic movement or purging of events on any basis, based on how you want to configure the system.

Security groups and permissions are easily set up in VideoManager EL, allowing you to grant individuals access to evidence on an as-needed basis.

Integration with In-Car and Body-Worn Cameras

Officers on the road are able to automatically upload encrypted video from in-car systems and body cameras. This eliminates the need for trips to and from the station solely for uploading data into the system.

Video and audio captured by M500, V300, 4RE and VISTA camera systems are automatically linked in VideoManager EL based on time and location. You can then utilize synchronized playback and export of video and audio from multiple devices in the same recording group, where video and audio streams can be matched together.

Optional Live Video Streaming

VideoManager EL integrates with SmartControl, an optional mobile application for Android and iOS that allows officers to review video evidence from their smartphone or tablet while they're still in the field.

SmartControl also allows officers to categorize recordings using event tags, stream live video from and change camera settings, such as adjusting field of view, brightness, and audio levels.

SmartConnect, an optional smartphone application, provides VISTA body-worn camera users with immediate in-field access to their body cameras. SmartConnect includes the ability to pair with VISTA cameras, adjust officer preferences, categorize recordings with incident IDs and case numbers, and play back recordings.

DEVICE MANAGEMENT

Agencies using VideoManager EL can assign users to devices, track them and streamline shift changes. You can easily manage, configure, update firmware and deploy in-car and body-worn cameras. Individual preference settings can be configured based on user profiles, allowing quick device transactions within a pooled or assigned device system. VideoManager EL also enables devices to be quickly exchanged between officers during shift changes. This minimizes the number of devices needed for your fleet.

Device Tracking

You can easily manage, configure and deploy your in-car and body-worn cameras in VideoManager EL. Devices can be assigned to personnel within VideoManager EL and tracked, helping agencies keep track of which users have specific devices.

Faster Shift Changes

VideoManager EL's Rapid Checkout Kiosk feature allows agencies using a pooled camera system to use fewer cameras. Cameras can be checked out at the start of a shift using an easy-to-use interface.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

At the end of the shift, the camera can be returned to its dock, where the video is automatically uploaded and the camera is made ready to be checked out and used for the next shift.

Devices can also be configured to remember individual preference settings for each user, including haptic and audible alert volume level, screen brightness and camera aim. These settings are applied whenever a device is assigned to a specific officer. A variety of settings within VideoManager EL also enable you to configure devices to operate in alignment with your agency’s policies and procedures.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

MOBILE VIDEO PRODUCTS NEW SYSTEM STATEMENT OF WORK

OVERVIEW

This Statement of Work (SOW) outlines the responsibilities of Motorola Solutions, Inc. (Motorola) and the Customer for the implementation of body-worn camera(s) and/or in-car video system(s) and your digital evidence management solution. For the purpose of this SOW, the term “Motorola” may refer to our affiliates, subcontractors, or certified third-party partners. A third-party partner(s) (Motorola-certified installer) will work on Motorola’s behalf to install your in-car video system(s) (if applicable).

This SOW addresses the responsibilities of Motorola and the Customer that are relevant to the implementation of the hardware and software components listed in the Solutions Description. Any changes or deviations from this SOW must be mutually agreed upon by Motorola and the Customer and will be addressed in accordance with the change provisions of the Contract. The Customer acknowledges any changes or deviations from this SOW may incur additional cost.

Motorola and the Customer will work to complete their respective responsibilities in accordance with the Project Schedule. Any changes to the Project Schedule must be mutually agreed upon by both parties in accordance with the change provisions of the Contract.

Unless specifically stated, Motorola will perform the work remotely. The Customer will provide Motorola personnel with access to their network and facilities so Motorola is able to fulfill its obligations. All work will be performed during normal business hours based on the Customer’s time zone (Monday through Friday from 8:00 a.m. to 5:00 p.m.).

The number and type of software subscription licenses, products, or services provided by Motorola are specifically listed in the Contract and referenced in the SOW. Services provided under this SOW are governed by the mutually executed Contract between the parties, or Motorola’s Master Customer Agreement and applicable addenda (“Contract”).

AWARD, ADMINISTRATION, AND PROJECT INITIATION

Project Initiation and Planning will begin following the execution of the Contract between Motorola and the Customer. At the conclusion of Project Planning, Motorola’s Project Manager (PM) will begin status meetings and provide status reports on a regular cadence with the Customer’s PM. The status report will provide a summary of activities completed, activities planned, progress against the project schedule, items of concern requiring attention, as well as, potential project risks and agreed upon mitigation actions.

Motorola utilizes Google Meet as its teleconference tool. If the Customer desires to use an alternative teleconferencing tool, any costs incurred from the use of this alternate teleconferencing tool will be the responsibility of the Customer.

FBI-CJIS SECURITY POLICY – CRIMINAL JUSTICE INFORMATION

CJIS Security Policy Compliance

Motorola does not believe our Mobile Video offerings (i.e. in-car/body-worn cameras) require compliance with the FBI-CJIS Security Policy (CJISSECPOL) based on the definition in Section 4 of CJISSECPOL and how the FBI-CJIS defines Criminal Justice Information. However, Motorola does design its products with the CJISSECPOL

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

security controls as a guide. Motorola's Mobile Video system design and features support best practice security controls and policy compliance. In the event of a CJIS technical audit request, Motorola will support the Customer throughout this process.

Personnel Security – Background Screening

Motorola will assist the Customer with completing the CJIS Security Policy Section 5.12 Personnel Security related to authorized personnel background screening when requested to do so by the Customer. Based on Section 5.12, a Motorola employee is defined as someone who is required to be on the Customer's property with unescorted access. Motorola employees will also have access to the Customer's network(s) and stored information. Motorola has remote access tools to support virtual escorted access to on-premises customer assets.

Additionally, Motorola performs independent criminal background investigations including name based background checks, credential and educational vetting, credit checks, U.S. citizen and authorized worker identity verification on its employees.

Motorola will support the Customer in the event of a CJIS audit request to validate employees assigned to the project requiring CJIS Section 5.12 Personnel Security screening and determine whether this list is up to date and accurate. Motorola will notify the Customer within 24 hours or next business day of a personnel status change.

Security Awareness Training

Motorola requires all employees who will support the Customer to undergo Level 3 Security Awareness Training provided by Peak Performance and their CJIS online training platform. If the Customer does not have access to these records, Motorola can facilitate proof of completion. If the Customer requires additional and/or separate training, Motorola will work with the Customer to accommodate this request at an additional cost.

CJIS Security Addendum

Motorola requires all employees directly supporting the Customer to sign the CJIS Security Addendum if required to do so by the Customer.

Third Party Installer

The Motorola-certified third party installer will work independently with the Customer to complete the Section 5.12 Personnel Security checks, complete Security Awareness Training and execute the CJIS Security Addendum.

COMPLETION CRITERIA

The project is considered complete once Motorola has completed all responsibilities listed in this SOW. The Customer's task completion will occur based on the Project Schedule to ensure Motorola is able to complete all tasks without delays. Motorola will not be held liable for project delays due to incomplete Customer tasks.

The Customer must provide Motorola with written notification if they do not accept the completion of Motorola responsibilities. Written notification must be provided to Motorola within ten (10) business days of task completion. The project will be deemed accepted if no written notification is received within ten (10) business days.

In the absence of written notification for non-acceptance, beneficial use will occur thirty (30) days after functional demonstration of the system.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

SUBSCRIPTION SERVICE PERIOD

If the contracted system includes a subscription, the subscription service period will begin upon the Customer's receipt of credentials for access. The provision and use of the subscription service is governed by the Contract.

PROJECT ROLES AND RESPONSIBILITIES OVERVIEW

Motorola Project Roles and Responsibilities

The Motorola Project Team will be assigned to the project under the direction of the Motorola PM. Each team member will be engaged in different phases of the project as necessary. Some team members will be multi-disciplinary and may fulfill more than one role.

In order to maximize effectiveness, the Motorola Project Team will provide various services remotely by teleconference, web-conference, or other remote method in order to fulfill our commitments as outlined in this SOW.

Our experience has shown customers who take an active role in the operational and educational process of their system realize user adoption sooner and achieve higher levels of success with system operation. The subsections below provide an overview of each Motorola Project Team Member.

Project Manager (PM)

The PM will be the principal business representative and point of contact for Motorola. The PM's responsibilities may include but are not limited to:

- Manage Motorola responsibilities related to the delivery of the project.
- Maintain the Project Schedule, and manage assigned Motorola personnel, subcontractors, and suppliers as applicable.
- Coordinate schedules of assigned Motorola personnel, subcontractors, and suppliers as applicable.
- Conduct equipment inventory if applicable.
- Maintain project communications with the Customer.
- Identify and manage project risks.
- Coordinate collaboration of Customer resources to minimize project delays.
- Evaluate project status against Project Schedule.
- Conduct status meetings on mutually agreed upon dates to discuss project status.
- Provide timely responses to Customer inquiries and issues related to project progress.
- Conduct daily status calls with the Customer during Go-Live.

Post Sales Engineer

The Post Sales Engineer will work with the Customer's Project Team on:

- Discovery validation.
- System provisioning.
- Covers the IT portion of the Project Kickoff Call with the Customer.
- Contracted data migration between two disparate digital evidence management systems (if applicable).

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

System Technologist (ST)

The ST will work with the Customer's Project Team on:

- Configure Customer's digital evidence management system.
- Inspect installation and configure hardware devices.
- Provide instructions to the Customer on how to configure the hardware.
- Review Deployment Checklist with the Customer.
- Develop and submit a Trip Report.
- Update Customer IP Map.

Professional Services Engineer (if applicable)

The Professional Services Engineer is engaged on projects that include integration between Motorola's digital evidence management system and the Customer's third-party software application. Their responsibilities include:

- Delivery of the interface between Motorola's digital evidence management system and the Customer's third-party software (e.g. CAD).
- Work with the Customer to access required systems/data.

Application Specialist (if applicable)

The Application Specialist will work with the Customer Project Team on system provisioning and education. The Application Specialist's responsibilities include but are not limited to:

- Deliver provisioning education and guidance to the Customer for operating and maintaining their system.
- Provide product education as defined by this SOW and described in the Education Plan.
- Provide on-site training based on the products the Customer purchased.

Technical Trainer / Instructor

The Technical Trainer / Instructor provides training on-site or remote depending on the training topic and deployment services purchased.

Motorola-Certified Installer

The Motorola-certified installer is primarily responsible for installing in-car video systems (ICVs) into Customer vehicles. There are specific requirements the 3rd party partner must meet in order to be considered a Motorola-certified installer, and they include the following:

- **Required Training**
  - WTG0501 - M500 Vehicle Installation Certification (Remote) or WTG0503 - M500 Vehicle Installation Certification (Live)
    - Needs to be renewed yearly.
    - Needs to be submitted to the PM by the technician completing the installation no less than thirty (30) days prior to the installation.
  - Review of any previous Motorola Solutions Technical Notifications (MTNs).
- **Optional Training**
  - WGD00186 - M500 Installation Overview and Quick Start (NA)
    - Not required for installation. Available for the installing technician.
  - WGD00177 - M500 In-Car Video System Installation Guide
    - Not required for installation. Available for the installing technician.
  - MN010272A01 - M500 In-Car Video System Basic Service Manual

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

- Not required for installation. Available for the installing technician.

Other responsibilities the Motorola-certified installer may be involved in include the installation of cellular routers or Access Points. These activities will only be completed by Motorola if Motorola quotes these services; otherwise, the completion of these services are solely the responsibility of the Customer.

Customer Support Services Team

The Customer Support Services Team will provide on-going support to the Customer following Go-Live and final acceptance of the project.

Customer Project Roles and Responsibilities

Motorola has defined key resources that are critical to this project and must participate in all the activities defined in this SOW. During the Project Planning phase, the Customer will be required to provide names and contact information for the roles listed below. It is critical that these resources are empowered to make decisions based on the Customer's operational and administration needs. The Customer Project Team will be engaged from Project Initiation through Beneficial Use of the system. In the event the Customer is unable to provide the resources identified in this section, Motorola may be able to supplement these resources at an additional cost.

Project Manager

The PM will act as the primary point of contact for the duration of the project. In the event the project involves multiple locations, Motorola will work exclusively with the Customer's primary PM. The PM's responsibilities will include, but are not limited to:

- Communicate and coordinate with other project participants.
- Manage the Customer Project Team including subcontractors and third-party vendors. This includes timely facilitation of tasks and activities.
- Maintain project communications with the Motorola PM.
- Identify tasks required of Customer staff that are outlined in this SOW and the Project Schedule.
- Consolidate all project inquiries from Customer staff to present to Motorola PM.
- Approve a deployment date offered by Motorola.
- Review Project Schedule with the Motorola PM and finalize tasks, dates, and responsibilities.
- Measure and evaluate progress against the Project Schedule.
- Monitor project to ensure resources are available as required.
- Attend status meetings.
- Provide timely responses to issues related to project progress.
- Liaise and coordinate with other agencies, Customer vendors, contractors, and common carriers.
- Review and administer change control procedures, hardware and software certification, and all related project tasks required to meet the deployment date.
- Ensure Customer vendors' readiness ahead of the deployment date.
- Assign one or more personnel to work with Motorola staff as needed for the duration of the project, including one or more representatives from the IT department.
- Identify a resource with authority to formally acknowledge and approve milestone recognition certificates, as well as, approve and release payments in a timely manner.
- Provide Motorola personnel with access to all Customer facilities where system equipment is to be installed. Temporary identification cards are to be issued to Motorola personnel, if required for access.
- Ensure remote network connectivity and access for Motorola resources.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

- Assume responsibility for all fees pertaining to licenses, inspections and any delays associated with inspections due to required permits as applicable to this project.
- Provide reasonable care to prevent equipment exposure from contaminants that may cause damage to the equipment or interruption of service.
- Ensure a safe working environment for Motorola personnel.
- Identify and manage project risks.
- Provide signature(s) of Motorola-provided milestone recognition certificate(s) within ten (10) business days of receipt.

IT Support

IT Support manages the technical efforts and ongoing activities of the Customer's system. IT Support will be responsible for managing Customer provisioning and providing Motorola with the required information for LAN, WAN, server and client infrastructure.

The IT Support Team responsibilities include but are not limited to:

- Participate in delivery and training activities to understand the software and functionality of the system.
- Participate with Customer Subject Matter Experts (SMEs) during the provisioning process and associated training.
- Authorize global provisioning decisions and be the Point of Contact (POC) for reporting and verifying problems.
- Maintain provisioning.
- Implement changes to Customer infrastructure in support of the proposed system.

Video Management Point of Contact (POC)

The Video Manager POC will educate users on digital media policy, participate in Discovery tasks, and complete the Video Management Administration training. The Customer is responsible for its own creation and enforcement of media protection policies and procedures for any digital media created, extracted, or downloaded from the digital evidence management system.

Subject Matter Experts (SMEs)

SMEs are a core group of users involved with the analysis, training and provisioning process, including making decisions on global provisioning. The SMEs should be experienced users in their own respective field (evidence, dispatch, patrol, etc.) and should be empowered by the Customer to make decisions based on provisioning, workflows, and department policies related to the proposed system.

Training POC

The Training POC will act as the course facilitator and is considered the Customer's educational monitor. The Training POC will work with Motorola when policy and procedural questions arise. They will be responsible for developing any agency specific training material(s) and configuring new users on the Motorola Learning eXperience Portal (LXP) system. This role will serve as the first line of support during Go-Live for the Customer's end users.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

General Customer Responsibilities (if applicable)

In addition to the Customer responsibilities listed above, the Customer is responsible for the following:

- All Customer-provided equipment, including third-party hardware and software needed for the proposed system but not listed as a Motorola deliverable. Examples include end user workstations, network equipment, etc.
- Configure, test, and maintain third-party system(s) that will interface with the proposed system.
- Establish an Application Programming Interface (API) for applicable third-party system(s) and provide documentation that describes the integration to the Motorola system.
- Coordinate and facilitate communication between Motorola and Customer third-party vendor(s) as required.
- Motorola-certified installers must be certified through LXP for remote or in person installation training. The Customer is responsible for work performed by non-certified installers.
- Upgrades to Customer's existing system(s) in order to support the proposed system.
- Mitigate the impact of upgrading Customer third-party system(s) that will integrate with the proposed system. Motorola strongly recommends working with the Motorola Project Team to understand the impact of such upgrades prior to taking action.
- Active participation of Customer SMEs during the course of the project.
- Electronic versions of any documentation associated with business processes identified.
- Providing a facility with the required computer and audio-visual equipment for training and work sessions.
- Ability to participate in remote project meetings using Google Meet or a mutually agreed upon Customer-provided remote conferencing tool.

Motorola is not responsible for any delays that arise from Customer's failure to perform the responsibilities outlined in this SOW or delays caused by Customer's third-party vendor(s) or subcontractor(s).

NETWORK AND HARDWARE REQUIREMENTS

The following requirements must be met by the Customer prior to Motorola installing the proposed system:

- Provide network connectivity for the transfer and exchange of data for the proposed system.
- Provide Virtual Private Network (VPN) remote access for Motorola personnel to configure the system and conduct diagnostics.
- Provide Internet access to server(s).
- Provide devices such as workstations, tablets, and smartphones with Internet access for system usage. Chrome is the recommended browser for optimal performance. The workstations must support MS Windows 11 Enterprise.
- Provide and install antivirus software for workstation(s).
- Provide Motorola with administrative rights to Active Directory for the purpose of installation, configuration, and support.
- Provide all environmental conditions such as power, uninterruptible power sources (UPS), HVAC, firewall and network requirements.
- Ensure required traffic is routed through Customer's firewall.

Motorola is not responsible for any costs or delays that arise from Customer's failure to meet network and hardware requirements.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

PROJECT PLANNING

A clear understanding of the needs and expectations of Motorola and the Customer is critical to fostering a collaborative environment of trust and mutual respect. Project Planning requires the gathering of specific information to set clear project expectations and guidelines, as well as lay the foundation for a successful implementation.

PROJECT PLANNING SESSION

A Project Planning Session will be scheduled after the Contract has been executed. The Project Planning Session is an opportunity for the Motorola and Customer PM to meet prior to the Project Kickoff Meeting and review key elements of the project and expectations. Depending on the items purchased, the agenda will typically include:

- A high level review of the following project elements:
  - Contract documents.
  - A summary of contracted applications and hardware as purchased.
  - Customer's involvement in project activities to confirm understanding of scope and required time commitments.
  - A high level Project Schedule with milestones and dates.
- Confirm CJIS background investigations and fingerprint requirements for Motorola employees and/or subcontractors.
- Determine Customer location for Motorola to ship their equipment for installation.

Motorola Responsibilities

- Schedule the remote Project Planning Session.
- Request the assignment of Customer Project Team and any additional Customer resources that are instrumental to the project's success.
- Provide the initial Project Schedule.
- Baseline the Project Schedule.
- Review Motorola's delivery approach and its reliance on Customer-provided remote access.
- Document mutually agreed upon Project Kickoff Meeting Agenda.
- Request user information required to establish the Customer in LXP.

Customer Responsibilities

- Identify Customer Project Team and any additional Customer resources that are instrumental to the project's success.
- Acknowledge the mutually agreed upon Project Kickoff Meeting Agenda.
- Provide approval to proceed with the Project Kickoff Meeting.

Motorola Deliverables

- Project Kickoff Meeting Agenda.

PROJECT KICKOFF

Motorola will work with the Customer to understand the impact of introducing a new solution and the preparedness needed for a successful implementation.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Note – The IT Questionnaire is completed during the pre-sales process and prior to Contract award. The IT Questionnaire is given to Motorola at the time of offer acceptance. Delay in completing the IT Questionnaire may delay shipment of equipment. Motorola will not be responsible for any delays associated with or related to the completion of the IT Questionnaire.

Motorola Responsibilities

- Review Contract documents including project delivery requirements as described in this SOW.
- Discuss the deployment start date and deliver the Deployment Checklist.
- Discuss vehicle equipment installation activities and responsibilities.
- Discuss the equipment inventory process (if applicable).
- Discuss project team participants and their role(s) in the project with fulfilling the obligations of this SOW.
- Review resource and scheduling requirements.
- Discuss Motorola remote system access requirements (24-hour access to a secured two-way Internet connection through the Customer's firewall for the purpose of deployment and maintenance).
- Discuss and deliver the Business Process Review (BPR) Workbook.
- Complete all necessary documentation (i.e. fingerprints, background checks, card keys, etc.) required for Motorola resources to gain access to Customer facilities.
- Discuss the LXP training approach.
- Provide designated Customer administrator with access to LXP.
- Review and agree on completion criteria and the process for transitioning to support.

Customer Responsibilities

- Provide feedback on project delivery requirements.
- Review the Deployment Checklist.
- Review the roles of project participants to identify decision-making authority.
- Provide VPN access to Motorola personnel to facilitate delivery of services described in this SOW.
- Validate non-disclosure agreements, approvals, and other related items are complete (if applicable).
- Provide all documentation (i.e. fingerprints, background checks, card keys, etc.) required for Motorola resources to gain access to Customer facilities.
- Provide Motorola with names and contact information to the designated LXP Administrator(s).

Motorola Deliverables

- Project Kickoff Meeting Minutes.
- BPR Workbook.
- Deployment Checklist.

DISCOVERY TELECONFERENCE

During the Discovery Teleconference, Motorola will meet with the Customer to define system configuration, as well as, agency recording and retention policies. This information will be documented in the Business Process Review (BPR) Workbook, which is used as a guide for configuration and provisioning decisions.

Motorola Responsibilities

- Facilitate Discovery Teleconference(s).
- Review and complete BPR Workbook with the Customer.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

- Confirm Customer-provided configuration inputs.

Customer Responsibilities

- Gather and review information required to complete the BPR Workbook during the Discovery Teleconference.
- Schedule Customer Project Team and SMEs to attend the Discovery Teleconference. SMEs should be present to weigh-in on hardware, software and network components. Customer attendees should be empowered to convey policies and make modifications to policies as necessary.
- Return completed BPR Workbook no later than five (5) business days after the conclusion of the Discovery Teleconference.

Motorola Deliverables

- Completed BPR Workbook.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

PROJECT EXECUTION

HARDWARE PROCUREMENT AND INSTALLATION

Motorola will procure contracted hardware as part of the ordering process. The hardware will be configured with a basic profile in line with the information provided by the IT Questionnaire or Discovery Teleconference for installation and configuration of the system. The Customer is responsible for providing an installation environment that meets manufacturer's specifications for the hardware, which includes but is not limited to:

- Power
- Heating and Cooling
- Network Connectivity
- Access and Security
- Conduit and Cabling

Motorola Responsibilities

- Procure contracted equipment and ship to the Customer's designated location.
- Inventory equipment after arrival at Customer location (if applicable).
- Install backend server in Customer's designated area (if applicable).
- Conduct a power-on test to validate the installed hardware and software are ready for configuration.
- Verify remote connection to hardware.
- For an on-site deployment, Motorola will be responsible for verifying the body-worn camera Transfer Stations are connected to the Customer's network. The Customer is responsible for ensuring Motorola has the correct IP address(es) for configuring the Transfer Stations, and the Customer's network is operational.
- The installer will be responsible for installing the Access Point(s) (APs) if provided by Motorola (if applicable).
- The ST will verify whether the AP(s) are properly installed and connected to the network (if applicable).
- Create a Trip Report outlining the activities completed during configuration and testing of system hardware.

Customer Responsibilities (if applicable)

- Procure Customer-provided equipment and make it available at the installation location.
- Confirm the server room complies with environmental requirements (i.e. power, uninterruptible power, surge protection, heating/cooling, etc.).
- Verify the server is connected to the Customer's network.
- Provide, install, and maintain antivirus software for server(s) and/or workstation(s).
- Enable outgoing network connection (external firewall) to the CommandCentral cloud by utilizing the Customer's Internet connection (if applicable).
- Install Customer-supplied APs (if applicable).
- Verify APs are properly installed and connected to the network (if applicable).
- For remote deployments, the Customer is responsible for verifying the body-worn camera Transfer Stations are connected to their network.
- Confirm access to installed software on Customer-provided workstation(s).
- For body-worn cameras, the Customer will verify whether the Transfer Station(s) are connected to their network.

Motorola Deliverables

- Contracted Equipment.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

- Equipment Inventory (if applicable).

In-Car Video System Configuration (if applicable)

The Motorola-certified installer will complete the installation of the in-car video (ICV) system(s) within the Customer-provided vehicle(s). The installer may also be responsible for installing cellular routers or WiFi radios inside the vehicle(s) for wireless upload of video to the Customer's digital evidence management system.

The Customer vehicles must be available for the ST to complete the configuration and testing of the contractual number of ICVs. If the Customer does not have all vehicles available during the agreed upon date and time, the Customer may opt to sign-off on the number of ICV configurations completed. If the Customer requires the ST to complete the full contractual number of ICVs at a later date and time, additional cost may be incurred. **Table 1-1** shows the number of ICVs an ST is contractually obligated to configure and test based on the number of ICVs purchased.

Table 1-1: Number of Contractual ICV Configurations

Number of ICV Purchased	Number of ICV to Test
1	1
2	2
3	3
4	4
5 - 25	5
26 - 50	10
51 - 75	15
76 - 100	20
101 - 150	30
151 - 200	40
201+	20%

Note – The Pricing Page will reflect in-car video installation services by Motorola if Motorola is responsible for the vehicle installations.

Motorola Responsibilities

- Setup server for ICV digital video recorder (DVR) configuration.
- Create configuration USB used to complete ICV hardware configuration and validation.
- Travel to the Customer site to conduct configuration and testing of ICVs.
- Complete ICV configuration on a single vehicle, and validate the configuration with the Customer.
- Receive Customer approval to proceed with remaining ICV configurations.
- Complete remaining contracted vehicle configurations.
- Test a subset of completed ICV hardware configurations.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

- For Motorola-certified installer, complete the installation of cellular router and confirm placement of antenna mounting with Customer (if applicable).
- The Motorola-certified installer will install Customer-provided SIM card into cellular router and connect cellular router to ICV (if applicable).
- Activities surrounding ICV (M500) interface to Automatic License Plate Recognition (ALPR) (if applicable).
  - Install Car Detector Mobile MDC Software on Customer-provided mobile data terminal (MDT) within the vehicle.
  - Configure MDC Network Card.

Customer Responsibilities

- Provide Motorola with remote connection and access credentials to complete ICV hardware configuration.
- Notify Motorola of the vehicle installation location.
- Coordinate and schedule date and time for ICV hardware configuration(s).
- Make ICV hardware available to Motorola for configuration and testing in accordance with the Project Schedule.
- Provide cellular SIM Card for Internet connectivity to the installer at time of vehicle installation.

Motorola Deliverables

- Complete Functional Validation Plan as it applies to the proposed solution.

NOTE - The Customer is responsible for having all vehicles and devices available for installation per the Project Schedule. All cellular data fees and Internet connectivity charges are the responsibility of the Customer. If a Motorola-certified installer is not used to install the ICV(s), Motorola is not responsible for any errors in hardware installation, performance or delays in the Project Schedule. In the event the Customer takes on the responsibility of installing the ICV(s) through a Motorola-certified installer, Motorola is also not responsible for any errors in hardware installation, performance or delays in the Project Schedule. For ALPR installations, an MDT is required for all vehicles (if applicable).

Body Worn Camera Configuration (if applicable)

The Transfer Station will be utilized to configure each body-worn camera according to the Business Process Review. In order for this process to be successfully completed, the Transfer Station must be connected to the Customer's digital evidence management system. The table below shows the number of body-worn cameras an ST is contractually obligated to configure and test based on the number of body-worn cameras purchased.

Table 1-2: Number of Contractual Body-Worn Camera Configurations

Number of BWC Purchased	Number of BWC to Test
1	1
2	2
3	3
4	4
5 - 25	5
26 - 50	10

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Number of BWC Purchased	Number of BWC to Test
51 - 75	15
76 - 100	20
101 - 150	30
151 - 200	40
201+	20%

Motorola Responsibilities

- Configure Transfer Station(s) for connectivity to the digital evidence management system.
- Verify the Transfer Station(s) is configured properly and connected to the network.
- Configure body-worn camera(s) within the digital evidence management system.
- Check out body-worn camera(s) and create a test recording.
- Verify completion of upload from body-worn camera(s) after it is docked in a Transfer Station or USB dock.
- Install and provide a demonstration of client software as part of the same on-site engagement as Go-Live, unless otherwise outlined in this SOW.

Customer Responsibilities

- Select physical location(s) for Transfer Station(s).
- Provide and install workstation hardware.
- Complete installation of client software on remaining workstations and mobile devices.
- Validate functionality of components and solution utilizing the Deployment Checklist.
- Provide Motorola remote connection information and necessary credentials.

Automatic License Plate Recognition (ALPR) Commissioning (if applicable)

This section highlights the responsibilities of Motorola and the Customer when an in-car video system interfaces with the Law Enforcement Archival Report Network (LEARN) database.

Motorola Responsibilities

- Create a Customer account in the LEARN system with user emails.
- Verify the Customer has installed and launched the Vigilant Car Detector Mobile Software per the Vigilant LEARN Quickstart Guide.
- Provide Mobile LPR - Officer Safety Basic and Advanced Pre-Installation Checklist.
- Provide Agency Manager with Training Materials and Car Detector Mobile MDC software installation guide.
- Advise Agency Manager of different options available to add new users.
- Confirm Agency Manager is aware of registration required for Hotlists.
- Confirm Agency Manager understands how to set up data-sharing.

Customer Responsibilities

- Identify the Agency Manager.
- Register to receive access to Hotlists.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

SOFTWARE INSTALLATION AND CONFIGURATION

Motorola will install VideoManager Evidence Library (EL) software on a specified number of workstations dictated by the Contract. The Customer will be responsible for installing the software on the remaining workstations. Provisioning of VideoManager EL software will be done in accordance with the information contained in the BPR Workbook.

Installation of VideoManager EL software consists of the following activities:

- Delivery and installation of server hardware (if applicable).
- Network discovery.
- Operating system and software installation.
- Onboarding user / group identity set up.
- Provide access to the application.

VideoManager EL (if applicable)

The VideoManager EL software is an on-premises solution that requires an onsite server and supports both body worn cameras and in-car video systems.

Motorola Responsibilities

- Install software on a specified number of customer workstations and/or mobile devices.
- Use information provided in the BPR Workbook to configure VideoManager EL software.
- Test software using applicable portions of the Functional Validation Plan.
- Provide instruction on client software USB utility.

Customer Responsibilities

- Provide a network environment that conforms to the requirements presented in the Solution Description.
- Procure and install server and storage hardware at desired location in accordance with Solution Description requirements.
- Perform a power on test with Motorola.
- Provide assigned Motorola System Administrator with access to SQL database for installation purposes (Motorola’s access will be revoked upon conclusion of the installation).
- For Active Directory integration, provide domain user (service account), security group (for application administrators including service account), and domain read access (if applicable).
- Provide workstation and/or mobile device hardware in accordance with specifications listed in the Solution Description.
- Complete online training.
- Complete installation of client software on remaining workstations and/or mobile devices.

VideoManager ELC (if applicable)

VideoManager ELC software is a cloud solution that does not require an onsite server and supports both body-worn cameras and in-car video systems.

Motorola Responsibilities

- Use information provided in BPR Workbook to configure VideoManager ELC software.
- Based on Customer feedback, perform the following activities:

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

  - Create users, groups, and setup permissions.
  - Create event categories.
  - Set retention policies.
- Test software using applicable portions of the Functional Validation Plan.
- Ensure training POC can access the system.

Customer Responsibilities

- Verify traffic can be routed through Customer's firewall and reaches end user workstations.

CloudConnect Installation and Configuration (applicable for CommandCentral Aware purchase)

Motorola Responsibilities

- Verify remote access capability.
- Remotely configure CloudConnect Virtual Machine within the Cloud Anchor Server.
- Configure network connectivity and test connection to the CloudConnect Virtual Machine.
- Create an IPSEC tunnel.
- Provide Customer with the information for setting up the IPSEC tunnel.

Customer Responsibilities

- Provide Motorola with two static IP addresses, corresponding subnet masks/default gateway, and available NTP and DNS IP for the CloudConnect Virtual Machine and the Cloud Anchor Server.
- Confirm with Motorola the network performance requirements are met.
- Configure firewall to allow traffic from IPSEC tunnel.

Completion Criteria

- CloudConnect Virtual Machine configuration is complete and accessible throughout the network.

CommandCentral Evidence (if applicable)

Motorola will work with the Customer to determine best industry practices, current operations environment, and subsystem integration to ensure optimal configuration of your CommandCentral Evidence solution.

Motorola Responsibilities

- Use the CommandCentral Admin Portal to provision users, groups, and rules based on Customer Active Directory data.
- Guide the Customer in the configuration of CommandCentral Evidence.

Customer Responsibilities

- Supply access and credentials to Customer's Active Directory for the purpose of Motorola conducting CommandCentral Evidence provisioning.
- Respond to Motorola's inquiries regarding users, groups and agency mapping to CommandCentral Evidence.
- Provision policies, procedures, and user permissions.
- Configure evidence as directed by Motorola.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

DATA MIGRATION SERVICES (IF APPLICABLE)

The Customer is responsible for partitioning data to be converted from a legacy or on-premises digital evidence management system to an on-cloud solution as part of this offer. The Customer will have ten (10) business days to provide feedback after Motorola validates the migrated data. If feedback is not received on or before ten (10) business days, Motorola will assume the migration is complete.

Motorola Responsibilities

- Receive access to Customer video data.
- Perform contracted data migration and validation.

Customer Responsibilities

- Provide remote access to partitioned data to be migrated.
- Validate migrated dataset, and provide Motorola with feedback within ten (10) business days.

Completion Criteria

- A migrated dataset as defined in the Contract.

DEMS INTEGRATIONS AND THIRD-PARTY INTERFACES (IF APPLICABLE)

The integration between Motorola's digital evidence management system and the Customer's third-party system may consist of an iterative series of activities depending on the complexity of accessing the third-party system. Interfaces will be installed and configured in accordance with the Project Schedule. The Customer is responsible for engaging third-party vendors as required to facilitate connectivity and testing of the interface(s).

Motorola Responsibilities

- Develop and configure interface(s) to support the functionality described in the Solution Description.
- Establish and validate connectivity between Motorola and third-party systems.
- Perform functional demonstration to confirm the interface(s) can transmit and receive data to the Customer's digital evidence management system.

Customer Responsibilities

- Act as liaison between Motorola and third-party vendor(s) as required to establish connectivity to the digital evidence management system.
- Provide personnel authorized to make changes to the network and third-party systems to support Motorola's integration efforts.
- Provide network connectivity between digital evidence management system and the third-party system(s).
- Provide information on API, SDKs, data scheme, and any documentation necessary to establish interfaces with all local and remote systems. This information should be provided to the Motorola PM within ten (10) business days of the Interface Engagement Meeting.

NOTE - At the time of initial design, unknown circumstances, requirements or anomalies may present difficulties with interfacing Motorola products to a third-party application. These difficulties could result in a poorly performing or a non-functional interface. By providing Motorola with this information early in the deployment process, will put us in the best position to mitigate these potential issues. If the resolution requires additional third-party integration, application upgrades, APIs, and/or additional software licenses, the Customer is responsible for addressing these issues at their cost. Motorola is not responsible for any delays or costs associated with third-party applications or Customer-provided third-party hardware or software.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

SYSTEM TRAINING

The objective of this section is to prepare for and deliver training. Motorola training consists of computer-based (online) and instructor-led (on-site or remote) depending on what is purchased. Our training delivery methods will vary depending on course content. Training will be delivered in accordance with the Education Plan. As part of our training delivery, Motorola will provide user guides and training materials in an electronic format.

ONLINE TRAINING (IF APPLICABLE)

Online training is made available to the Customer through LXP. This subscription service provides customers with unlimited access to our online training content and provides users with the flexibility of learning the content at their own pace. Training content is added and updated on a regular basis to keep information current.

Through LXP, a list of available online training courses, Motorola User Guides, and Training Material are accessible in electronic format.

Motorola Responsibilities

- Designate a LXP Administrator to work with the Customer.
- Establish an accessible instance of LXP for the Customer.
- Configure a Customer-specific portal view.
- Organize content to align with Customer's selected technologies.
- Create initial Customer user accounts and a single Primary Administrator account.
- During onboarding, assist the Customer with LXP usage.
- Provide technical support for user account and access issues, LXP functionality, and Motorola managed content.
- Provide instruction to Customer LXP Administrator on building groups.

Customer Responsibilities

- Provide user information for the initial creation of accounts.
- Complete LXP Administrator training.
- Ensure network and Internet connectivity for Customer access to LXP.
- Customer's primary LXP Administrator is required to complete the following self-paced training: LXP Introduction (LXP0001), LXP Primary Site Administrator Overview (LXP0002), and LXP Group Administrator Overview (LXP0003).
- Advise users on the availability of training through LXP.
- Ensure users complete LXP training in accordance with the Project Schedule.
- Build groups as needed.

INSTRUCTOR-LED TRAINING (ON-SITE AND REMOTE, IF APPLICABLE)

Instructor-led courses are based on products purchased and the Customer's Education Plan.

Motorola Responsibilities

- Deliver User Guides and training materials in an electronic format.
- Perform training in accordance with the Education Plan.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

- Provide the Customer with training attendance rosters and summarize any pertinent information that may impact end user training.

Customer Responsibilities

- Supply classroom(s) based on the requirements listed in the Education Plan.
- Designate training representatives who will work with the Motorola trainer(s) to deliver the training content.
- Facilitate training of all Customer end users in accordance with the Customer's Education Plan.

Motorola Deliverables

- Electronic versions of User Guides and training materials.
- Attendance rosters.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

PROJECT GO-LIVE, CLOSURE, AND HANDOVER TO SUPPORT

Motorola will utilize the Deployment Checklist throughout the deployment process to verify features and functionality are in line with installation and configuration requirements. The Customer will witness the ST demonstrating the Deployment Checklist and provide feedback as features and functionality are demonstrated. The Customer is considered Live on the system after the equipment has been installed, configured, and made available for use, and training has been delivered or made available to the Customer.

Upon the conclusion of Go-Live, the project is prepared for closure. Project closure is defined as the completion of tasks and the Customer's receipt of contracted components. The Deployment Checklist serves as the artifact that memorializes a project closure. A System Acceptance Certificate will be provided to the Customer for signature to formally close out the project. The Customer has ten (10) business days to provide Motorola with a signed System Acceptance Certificate. If the Customer does not sign off on this document or provide Motorola written notification rejecting project closure, the project will be deemed closed. Upon project closure, the Customer will engage with Technical Support for on-going needs in accordance with the Customer's specific terms and conditions of support.

Motorola Responsibilities

- Provide the Customer with Motorola Technical Support engagement process and contact information.
- Provide Technical Support with the contact information of Customer users who are authorized to engage Technical Support.
- Ensure Deployment Checklist is complete.
- Obtain Customer signature on the System Acceptance Certificate.
- Provide Customer survey upon closure of the project.

Customer Responsibilities

- Within ten (10) business days of receiving the System Acceptance Certificate, provide signatory approval signifying project closure.
- Provide Motorola with the contact information of users who are authorized to engage Motorola's Technical Support.
- Engage Technical Support as needed.

Motorola Completion Criteria

Provide Customer with survey upon closure of the project.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

ASSUMPTIONS

This SOW is based on the following list of assumptions (if applicable):

- Videomanager EL Cloud (VMELC) must be connected to the Microsoft Entra ID (formally known as Microsoft Azure Active Directory) for user authentication to the VMELC application. Microsoft Entra ID can be synchronized with the Customer's on-premises Active Directory using Azure AD Connect. If the Customer is using Microsoft Office 365, Motorola will be able to integrate with this Microsoft Entra ID.
- Must be 2003 or later for Microsoft Entra ID integration.
- Upload Speed Requirements for Hardware Devices
  - 5 Mbps + 3 Mbps per additional device.
    - This assumes it will take 8 hours to upload 5 GB of video on a device.
  - 40-50 Mbps per concurrent uploading device.
    - This assumes video is required to upload within 30-40 minutes with approximately 5 GB to upload.
- If the Customer is supplying an upload server to temporarily store video, please verify the server complies with the specifications provided in the Solutions Description.
- By default, M500 ICVs and V300/V700 BWCs do not need an upload server for cloud deployments. An upload server may be required depending on how many devices are uploading concurrently and the need for the Customer to upload video evidence at a given speed.
- Upload appliance required if using 4REs or VISTA body worn cameras connected to VideoManager EL Cloud
- Cellular upload of ICVs and BWCs (if applicable) requires an Ethernet connection to an LTE modem in the vehicle.
- If the Customer is supplying a server for VideoManager EL (On-premises) solution, the Customer must verify the server is not a Domain Controller.
- VideoManager EL for on-premises cannot be installed on a server running Active Directory or Exchange applications on the Customer’s network.
- The ICVs are configured with a hidden SSID and WPA2-AES Security with a 128-bit Pre-shared Key. If another type of security is desired, the Customer will be responsible for configuring these security requirements into the ICVs. This information must be supplied through the IT Questionnaire in order for the factory to configure the correct security requirements.
- If the Customer is supplying their own Access Point, it must be 5 GHz 802.11n compatible.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

V700 BODY-WORN CAMERA SOLUTION DESCRIPTION

The V700 body-worn camera captures clear video and audio of every encounter from the user's perspective. Its continuous-operation capabilities allow constant recording, helping the user to capture every detail of each situation and create a reliable library of evidence for case building and review. The V700 can stream live video and report real time GPS location through a built-in LTE modem, directly to the suite of CommandCentral applications.

The V700 is easy to operate, with four control buttons. Its innate Record-After-the-Fact® (RATF) technology enables the device to capture important video evidence that can be retrieved hours or days after an incident occurs, even if a recording is not triggered by the user or sensor. With RATF, officers can prioritize response to immediate threats versus manually activating their camera.

KEY FEATURES OF THE V700

- **Detachable Battery –** The V700's detachable battery allows officers to switch to a fully-charged battery if their shift goes longer than expected. Since the battery charges without being attached to the V700, the battery is kept fully charged in the dock ready for use. This feature is especially helpful for agencies that share body-worn cameras with multiple officers.
- **Wireless Uploading –** Recordings made by the V700 are uploaded to the agency's evidence management system via LTE or WiFi. This enables easy transfer of critical recordings to headquarters for immediate review or long-term storage.
- **Real-time Location and Video Streaming –** With built-in LTE connectivity, the V700 paired with CommandCentral Aware will send location updates and stream live video to a dispatch center or Real Time Crime Center (RTCC) giving the agency a complete and accurate view of their officers for better coordination and quicker response times.
- **LTE Service Ready –** The V700 is approved for use on Verizon and FirstNet networks in the U.S. and Bell Mobility in Canada. The V700 will ship with a pre-installed SIM from both carriers, ready for service activation upon arrival with a data plan that best suits the agency's needs. LTE service activation would be on the agency's carrier account.
- **Data Encryption –** The V700 uses FIPS-140-2 compliant encryption at-rest and in-transit. This ensures recordings made by the agency's officers are secure from unauthorized access.
- **Record-After-The-Fact® –** Our patented Record-After-the-Fact® technology captures footage even when the recording function is not engaged. The camera user or admin can request video footage from a specific point in the past to be uploaded to the evidence management system, hours or even days after the event occurred.
- **Natural Field of View –** The V700 eliminates the fisheye effect from wide-angle lenses that warps video footage. Distortion correction ensures a clear and complete evidence review process. The V700's high quality, low light sensor captures an accurate depiction of recorded events, even in challenging lighting conditions.
- **SmartControl Application –** To maximize efficiency in the field, the Motorola Solutions SmartControl app enables V700 users to preview video recordings, add or edit tags, change camera settings and view live video from the camera. The app is available for both iOS and Android phones.
- **In-Field Tagging –** The V700 enables easy in-field event tagging. It allows officers to view event tags and save them to the appropriate category directly from the body-worn camera or via the SmartControl app.
- **Auto Activation –** The V700 body-worn camera(s) paired with an M500 or 4RE in-car video system(s) can form a recording group, which automatically starts recording when one of the devices begins to record. Each device can be configured to initiate a group recording using triggers like lights, sirens, doors, gun racks, and other auxiliary inputs. Up to eight V700s can form a recording group and collaborate on recordings, without a

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

corresponding in-car video system, using similar triggers. Group recordings are uploaded and automatically linked to the evidence management system as part of one event.

V700 AND IN-CAR VIDEO INTEGRATION

The V700 integrates seamlessly with the M500 or 4RE in-car video systems, capturing video of an incident from multiple vantage points. This integration includes the following features:

- **Distributed Multi-Peer Recording –** Multiple V700 body-worn cameras and in-car video systems can form a recording group and based on the configuration, automatically start recording when one of the devices begins to record. Group recordings are uploaded and automatically linked to the evidence management system as part of one incident.
- **Automatic Tag Pairing –** Recordings captured by integrated V700 body-worn cameras and in-car video systems can be uploaded to the evidence management system with the same tags. From the in-car video system's display, videos can be saved under the appropriate tag category. The tag is then automatically shared with the V700 video and uploaded as part of one incident along with the officer's name.
- **Evidence Management Software –** When V700 body-worn cameras and in-car video systems record the same incident, the Motorola Solutions evidence management software automatically links those recordings based on officer name, date, and time overlap.
- **Additional Audio Source –** The V700 can serve as an additional audio source when integrated with the in-car video system. The V700 also provides an additional view of the incident and inherits the event properties of the in-car video system's record, such as officer name, event category, and more, based on configuration.
- V700 and APX Radio Integration

Motorola Solutions' APX two-way radios can pair with V700 body-worn cameras to automate video capture through Bluetooth. When the APX's emergency mode button is pressed, or the Man Down feature is activated, the V700 is triggered to start recording immediately. The recording will continue until manually stopped by the officer via the start/stop button on the V700 or group in-car video system.

HOLSTER AWARE™ INTEGRATION

The V700 integrates with a Holster AwareTM sensor through Bluetooth. If configured, the sensor automatically prompts the V700 to record the moment the holstered equipment is drawn. The holster sensor information is stored with the V700 user profile and uploaded to the evidence management system. If the user is assigned to a different camera, the holster sensor information will be applied to the new camera. The holster sensor allows officers to record high-stress events as they unfold, without having to sacrifice situational awareness by manually activating the V700.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

DOCKING STATIONS

The V700 has three docking options:



Transfer Station – The Transfer Station is built for large, multi-location agencies with large numbers of V700 cameras in service at any given time. It can charge up to eight fully assembled body-worn cameras or individual batteries. The eight docking slots include an LED indication of a battery charging and upload status. While the V700 charges, the Transfer Station can automatically offload recordings from the camera to the evidence management system via an integrated 2.5Gb switch. The Transfer Station connects directly to the LAN for fast offload of recorded events to storage, while charging the body-worn camera battery. The Transfer Station supports comprehensive device management capabilities, such as camera configuration, checkout and officer assignment options; rapid checkout, kiosk, and individual camera checkout; automatic firmware and configuration updates.



USB Base – The USB Base charges the battery of a single V700 or standalone battery pack. The USB Base can be mounted in a vehicle or attached to a desktop or Mobile Data Computer with 12V or USB connection for power. The USB Base has LED indications for battery charging status and upload, and an ambient light sensor for optimal LED brightness control from bright sunlight to the dim interior of a patrol car. When connected to a laptop or desktop computer, the USB Base can be used to upload recordings to the evidence management system, as well as, receive firmware and configuration updates.



Wi-Fi Base – The Wi-Fi Base is mounted in a vehicle. It facilitates V700 upload of video evidence to the evidence management system, firmware updates, communication between V700 and in-car video system group devices and charges fully assembled V700s or individual battery packs. It has LED indications of battery charging status and upload, and an ambient light sensor for optimal LED brightness control, from bright sunlight to the dim interior of a patrol car.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

MOUNTING SOLUTIONS

V700 is compatible with the entire line of V300 mounting solutions as depicted below.

WGP02798	WGA00669	WGA00668	WGP02697	WGP03088	WGP03085
					
Magnetic Center Shirt Mount	Tek-Lok Belt Mount	Molle Locking Mount	Shirt Clip	Heavy Jacket Clip	Heavy Jacket Magnetic Mount

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

STATEMENT OF WORK — ESSENTIAL SERVICE FOR V700 BODY WORN CAMERA DEVICE (NORTH AMERICA)

This Statement of Work ("SOW") is subject to the terms and conditions of the Motorola Solutions Service Agreement or other applicable agreement in effect between the parties ("Agreement"). The terms of this SOW are an integral part of an Agreement with the Customer to which this SOW is appended and is made a part thereof by this reference. In the event of a conflict between the terms and conditions of an Agreement and the terms and conditions of this SOW, this SOW will control the inconsistency only. This SOW applies to the Device(s) specifically named in the Agreement.

DESCRIPTION OF SERVICES AND OBLIGATIONS

The term "Customer" refers to any end-user who has a purchase agreement with Motorola Solutions.

Essential Service provides either three (3) or five (5) years of coverage, as selected by the Customer, and includes:

- Remote Technical Support
- Software Maintenance
- Software Enhancements
- Hardware Repair for manufacturing defects

Motorola Solutions includes three (3) years of Essential Service with each Body Worn Camera (BWC) device purchase, with optional service upgrades to extend and/or provide additional coverage for the device.

ESSENTIAL SERVICE

Remote Technical Support

Remote Technical Support is provided for device issues related to software and/or hardware that require troubleshooting expertise. Motorola Solutions' System Support Center (SSC) and Technical Support Operations (TSO) center are staffed with highly trained technologists who specialize in the diagnosis and resolution of product issues. Motorola Solutions' SSC and TSO are continuously monitored against stringent, industry recognized incident and problem management processes.

Motorola Solutions will respond to calls, e-mails, and web portal submissions during normal support hours, five (5) business days per week, excluding holidays, and weekends. In addition, Customers may contact the Motorola Service Desk and a Motorola Solutions representative will log a technical request on Motorola Solutions' Case Management System.

Technical Problem Isolation, Analysis and Resolution.

A Motorola Solutions representative or technologists will:

- Work to isolate the problem/issue
- Analyze and determine the cause of the problem/issue
- Work to achieve problem/issue resolution

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Software Maintenance

Software maintenance is important for ensuring device performance and operation. Essential Service provides the Customer with access to the latest available Body Worn Camera (BWC) device operating system (OS) software, device firmware, and application software. Device software releases maintain the device software performance such that the Device operates in accordance with its specifications and documented functionality, and is aligned with the applicable Motorola Solutions infrastructure platform lifecycle. Each release may include bug fixes, security patches, and/or new feature activation enablements.

Configuration of the Body Worn Camera (BWC) device is made possible through the use of the CommandCentral DEMS, VideoManager EL On-Premises, or VideoManager EL Cloud, solution.

Access to software updates will remain available until the expiration of the initial term of the Essential Service Package. Upon expiration of the initial Essential Service term, availability of software updates will terminate, unless the Customer renews Essential Service.

Software Enhancements

Software Enhancements are included with all BWC devices that have a valid Essential Service Package. Software Enhancements may include, or introduce, new device features, functionality, or capabilities, that were not available at time of device purchase. Availability of software enhancements depends on the device hardware and software capability to work with the new enhancements. Certain enhancements, not included with Essential Service Packages, may only be available as an additional purchase.

Motorola Solutions, at its discretion, reserves the right to add new software enhancements, or remove existing software enhancements, from any of its Essential Service Package. Please contact your Motorola Solutions Sales associate, or visit the Motorola Solutions' Web portal, for additional information regarding device features and capabilities.

Software Enhancements for the device will be continuously available until the expiration of the initial term of the Essential Service Package. Upon expiration of the initial term of Essential Service, availability of Software Enhancements will terminate, unless the Customer renews Essential Service.

Device Hardware Repair

Essential Service provides the Customer with repair services at a Motorola Solutions owned and operated, supervised, or certified Repair Center that employs the latest test equipment and original or certified replacement components used in the manufacturing of the BWC device. Device Hardware Repair provides the Customer with repair services for internal and external device components that are damaged as a result of manufacturing defects and defects due to normal wear and tear. With this Service, the device is repaired to ensure full compliance with its specifications, as published by Motorola Solutions at the time of delivery of the original device via:

- Repairs, adjustments and restorations, if appropriate, of any device that malfunctions while being used within the operational and environmental parameters specified by Motorola Solutions.
- Device updates, if applicable, as may be released, from time to time, by Motorola Solutions in accordance with an Engineering Change Notice.

At the discretion of Motorola Solutions, if the device is considered “un-repairable”, for technical or economic reasons, Motorola will replace the device with a new or refurbished device.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

A three (3) year optional Service is available for the Transfer Station. Scope includes Technical Support and Hardware Repair as described in sections 1.2.1 and 1.2.4.

Essential Software Service

If for any reason the Customer declines or chooses to exclude the hardware repair option that is included with the three (3) year Essential Service Package, the Customer will automatically default to, and be entitled to, three (3) years of Essential Software Service and one (1) year of hardware repair against manufacturing defects, as covered by the standard product warranty.

Essential Software Service provides three (3) years of coverage and includes:

- Remote Technical Support
- Software Maintenance
- Software Enhancements

Scope of Products or Services included

Essential Service, and optional Service upgrades, are currently available for all V700 Body Worn Camera devices. Check with your Motorola Solutions' Sales representative if you have a question about the eligibility of your device.

Optional and purchasable Services are available for the Transfer Station.

MOTOROLA SOLUTIONS RESPONSIBILITIES

Software Release Availability. Motorola Solutions will provide access to the latest BWC device software and firmware releases via the CommandCentral DEMS, VideoManager EL On-Premises, or VideoManager EL Cloud, solution. For customers using the CommandCentral DEMS or VideoManager EL Cloud, software and firmware upgrades will occur automatically when the Body Worn Camera device connects to the agency's CommandCentral DEMS or VideoManager EL Cloud instance. If using the VideoManger EL On-Premises solution, the on-prem server will periodically connect to the VideoManager EL Cloud database to check for new software and firmware versions, download the latest version, and apply the new software and/or firmware automatically to the BWC device when it connects to the server.

Software Release Notes. Motorola Solutions may, from time to time, provide release notes for the BWC Device software release. Information regarding training material will be posted on the Learning Experience Portal (LXP) at https://learning.motorolasolutions.com

Hardware Repair. Motorola Solutions will provide repair or replacement of a device, at its option, with a five (5) business day in-house turnaround time, provided the device is delivered to the repair center by 9:00 a.m. (local repair center time), and replacement parts, components, and/or devices are available. Business days do not include holidays or weekends. Repair may include the replacement of parts, or boards with new parts or complete boards or, at Motorola Solutions' option, with functionally equivalent, reconditioned parts, boards, or with a new or refurbished replacement device. All replaced parts, boards or devices will become the property of Motorola Solutions. Turnaround time represents the time a product spends in the repair process; it does not include time in transit, including customs clearance.

LTE/4G Service. Motorola Solutions supports the operation of the V700 BWC device on multiple approved LTE/4G Carrier Networks. Based on the Customer's selection of a Carrier during the initial ordering process,

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Motorola Solutions will install, in the device, the Customer's selected Carrier SIM, before the device is shipped to the Customer. The Customer is responsible for contacting the Carrier and activating the LTE/4G data service.

Shipping. For devices repaired under Essential Service, Motorola Solutions will provide one-way shipping, from an Authorized Motorola Repair Center to the Customer. The Customer is responsible for the shipping method and any shipping costs incurred when returning the faulty device to an Authorized Motorola Solutions repair center. Based on the country of purchase, Motorola Solutions may also cover, or include, two-way shipping for the damaged or defective device. Eligibility for two-way shipping will be confirmed during the repair submission process.

CUSTOMER RESPONSIBILITIES

Serial Numbers. If device orders are submitted via Motorola Solutions' Partner Hub, OCC, or CPQ ordering systems, the hardware serial number(s) for three (3) year Essential Service and Essential Software, as well as five (5) year Essential Service, and three (3) and five (5) year Essential Service with Accidental Damage and Advanced Replacement, will be automatically captured and included in the Service Agreement.

If five (5) year Essential Service or three (3) and five (5) year Essential Service with Accidental Damage and Advanced Replacement is purchased within 90 days of device shipment, the Customer must provide a complete list, preferably in electronic format, or by completing a Service Order Form (SOF), of all hardware serial numbers to be covered under the Agreement.

Initiating Repair. When initiating a repair, the Customer must contact Motorola Solutions to obtain a Return Material Authorization (RMA) number for each faulty BWC device. The Customer can submit a repair, and request an RMA, via the Partner Hub Portal, or by contacting the Motorola Solutions' Service Desk. If two-way shipping is included, the customer can generate a shipping label via Partner Hub, or by contacting the Motorola Solutions Service Desk. The Return Material Authorization (RMA) must be included with the device when shipped to the Authorized Motorola Repair Center.

- Only the BWC device should be returned for repair. The battery must be removed before shipping the device to a Motorola Solutions Repair Center.
- Device accessories should not be included when returning a device to a Motorola Solutions Repair Center for repair. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.
- The SIM card must remain in the device, and intact, when the device is shipped to a Motorola Solutions Repair Center. If the SIM card is removed, or if any evidence of SIM card tampering is found, including disassembling of the device, the warranty will be null and void.

Motorola Solutions is not responsible for any accessories, or device batteries, that are shipped with the device for repair.

Device software releases. The Customer will be responsible for updating each eligible BWC device with the latest available software and/or firmware, and of advising users of any operational changes that may have been introduced as a result of the new software or firmware.

LTE/4G Service. The Customer is responsible for selecting a Motorola Solutions approved LTE/4G Carrier/Provider during the initial ordering process, and for contacting the Carrier and activating LTE service for the device. The Customer is solely responsible for all financial obligations with the selected LTE Carrier.

Wi-Fi Connectivity. The Customer is responsible for providing all Wi-Fi connectivity to the device.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Removing Customer Data. The Customer is responsible for removing, from the device, any data, video, or other information that the Customer wishes to retain or destroy, prior to sending the device to a Motorola Solutions Repair Center for repair.

Motorola Solutions may provide a Video Evidence Recovery Service for the BWC device, as an additional charge. Video Evidence Recovery is a best effort service that is dependent on the condition of the device. This service, if applicable, will have a separated Agreement, with Terms and Conditions, outside the scope of this Statement of Work (SOW). Please contact your Motorola Solutions Representative for more information regarding the Video Evidence Recovery Service.

ESSENTIAL SERVICE LIMITATIONS AND RESTRICTIONS

Customer will incur additional charges at the prevailing rates for any of the following activities, which are not covered under this Agreement:

- Replacement of consumable parts or accessories, as defined by product, including but not limited to batteries, cables, mounts, or clips.
- Repair of problems caused by natural or manmade disasters, including but not limited to fire, theft and floods that would cause internal or external component damage or destruction.
- Repair of problems caused by third parties' Software, accessories or peripherals not approved in writing by Motorola Solutions for use with the device.
- Repair of problems caused by using the device outside of the product's operational and environmental specifications, including improper handling, carelessness or reckless use, or repaired by a third party.
- Repair of problems caused by unauthorized alterations or attempted repair.
- Non-remedial work, including but not limited to administration and operator procedures, reprogramming, and operator or user training.
- Problem determination and/or work performed to repair or resolve issues with non-covered products; for example, any hardware or software products not specifically listed on the service order form.
- Any file or video backup or restoration.
- Completion and test of incomplete application programming or system integration if not performed by Motorola Solutions and specifically listed as covered.
- Use of Software or Firmware releases, except as provided for under the responsibilities outlined in this document.
- Accidental damage, chemical or liquid damage, or other damage caused outside of normal device operating specifications, unless the Customer has purchased the optional Essential Service with Accidental Damage and Advanced Replacement package.
- Cosmetic imperfections that do not affect the functionality of the device.

Where a Body Worn Camera device is submitted for repair that is outside the scope of Service, such repair may be quoted by Motorola Solutions for additional cost in accordance with Motorola Solutions' standard Time and Materials (T&M) rates and terms and conditions. Motorola Solutions will notify the Customer of any incremental charges related to the aforementioned exclusions prior to completing the repair and said repair will be subject to acceptance of the quotation by the Customer.

Software support for unauthorized modifications, or other misuse of the device software, is not covered under this Agreement.

Access to the software and firmware releases for updating the device under this SOW is available only for the device named in the Agreement. Software updates to any additional devices are expressly excluded and

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

prohibited. Notwithstanding the foregoing, Motorola Solutions may, at its sole discretion, include coverage for other devices.

Any implementation tools not required to support the device software and firmware updates are excluded from coverage.

MOTOROLA SOLUTIONS IS NOT OBLIGATED TO PROVIDE SUPPORT FOR ANY DEVICE:

- That has been repaired, tampered with, altered or modified (including the unauthorized installation of any software) — except by Motorola Solutions authorized service personnel.
- That has been subjected to unusual physical or electrical stress, abuse, or forces or exposure beyond normal use within the specified operational and environmental parameters set forth in the applicable product specification.
- If Customer fails to comply with the obligations contained in the product purchase agreement and/or the applicable software license agreement and/or Motorola Solutions terms and conditions of service.

ESSENTIAL SERVICE WITH ACCIDENTAL DAMAGE REPAIR AND ADVANCED REPLACEMENT

Description of Services and Obligations

Accidental Damage coverage is an optional, prepaid service that adds coverage for accidentally damaged BWC devices. Accidental Damage coverage must be purchased together with, or within 90 days of, a qualifying Motorola Solutions device purchase. This three (3) or five (5) year service offer reduces unexpected expenses related to the repair of the device. Accidental Damage and Advanced Replacement coverage includes all services provided under Essential Service, plus additional coverage for Accidental Damage and Advanced Replacement of the damaged device.

Examples of repairs covered under Accidental Damage include:

- Electrical repair for failures caused by accidental water or chemical damage
- Electrical repair for accidental internal damage
- Replacement of accidentally cracked or broken housings.
- Replacement of accidentally cracked or broken camera lens or displays.
- Replacement of accidentally cracked or broken or missing buttons, knobs, or keypads

Repair or Replacement. Motorola Solutions will provide repair or replacement of a BWC device, at its option, with a five (5) business day in-house turnaround time, excluding weekends and holidays, provided the device is delivered to the repair center by 9:00 a.m. (local repair center time), and replacement parts, components, and/or devices are available. Repair may include the replacement of parts, or boards with new parts or complete boards or, at Motorola Solutions option, with functionally equivalent, reconditioned parts, boards, or with a new replacement or refurbished device. All replaced parts, boards or devices will become the property of Motorola Solutions. Turnaround time represents the time a product spends in the repair process; it does not include time in transit, including customs clearance.

Serial Numbers. If the Accidental Damage Service is purchased with the device, in the same order, using Motorola Solutions' Partner Hub Portal, OCc, or CPQ when ordering, the hardware serial number(s) are automatically captured and included in the Service Agreement. If Accidental Damage Service is purchased within 90 days of device shipment, the Customer must provide a complete list, preferably in electronic format, or by completing a Service Order Form (SOF), of all hardware serial numbers to be covered under the Agreement.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

Initiating Repair. When initiating a repair, the Customer must contact Motorola Solutions to obtain a Return Material Authorization (RMA) number for each faulty BWC device. The Customer can submit a repair, and request an RMA, via the Partner Hub Portal, or by contacting the Motorola Solutions' Service Desk. If two-way shipping is included, the customer can generate a shipping label via Partner Hub, or by contacting the Motorola Solutions Service Desk. The Return Material Authorization (RMA) must be included with the device when shipped to the Authorized Motorola Repair Center.

- Only the BWC device should be returned for repair. The battery must be removed before shipping the device to a Motorola Solutions Repair Center.
- Device accessories should not be included when returning a device to a Motorola Solutions Repair Center for repair. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.
- The SIM card must remain in the device, and intact, when the device is shipped to a Motorola Solutions Repair Center. If the SIM card is removed, or if any evidence of SIM card tampering is found, including disassembling of the device, the warranty will be null and void.

Motorola Solutions is not responsible for any accessories, or device batteries, that are shipped with the device for repair.

Advanced Replacement. Under Accidental Damage and Advanced Replacement Service, Motorola Solutions will provide Advanced Replacement for the damaged device. Motorola Solutions will ship a new or refurbished replacement device to the Customer within two (2) business days of receiving the Customer repair request, subject to availability of replacement devices. Business days do not include weekends or holidays.

The Customer must return the defective or damaged device to a Motorola Solutions Repair Center within 30 days after receiving the replacement device. Failure to return the damaged device to Motorola Solutions will result in an additional Customer charge for the replacement device.

When returning a device for Advanced Replacement, device accessories should not be included. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.

Motorola Solutions is not responsible for any accessories that are shipped with the device.

ACCIDENTAL DAMAGE AND ADVANCED REPLACEMENT LIMITATIONS AND RESTRICTIONS

Customer will incur additional charges at the prevailing rates for any of the following activities, which are not covered under this Agreement:

- Replacement of consumable parts or accessories, as defined by product, including but not limited to batteries, chargers, charging stations, mounts, and clips.
- Repair of problems caused by natural or manmade disasters, including but not limited to fire, theft and floods that would cause internal or external component damage or destruction.
- Repair of problems caused by third parties' Software, accessories or peripherals not approved in writing by Motorola Solutions for use with the device.
- Repair of problems caused by using the device outside of the product's operational and environmental specifications, including improper handling, carelessness or reckless use, or repair by a third party.
- Repair of problems caused by unauthorized alterations or attempted repair.
- Non-remedial work, including but not limited to administration and operator procedures, reprogramming, and operator or user training.
- Problem determination and/or work performed to repair or resolve issues with non-covered products; for example, any hardware or software products not specifically listed on the service order form.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

- Any file or video backup or restoration.
- Completion and test of incomplete application programming or system integration if not performed by Motorola Solutions and specifically listed as covered.
- Use of Software or Firmware releases except as provided for under the responsibilities outlined in this document.

There is a maximum limit of one (1) Body Worn Camera device repair, per contract year, for Essential Service with Accidental Damage and Advanced Replacement.

Where ongoing “Accidental Damage” repair is deemed by Motorola Solutions to be excessive, systemic, or the result of device mishandling, the Customer may be subject to an additional charge. Should the accidental damage continue unabated, the Customer will incur repair charges at Motorola Solutions’ discretion and prevailing charges for devices deemed by Motorola Solutions to have been damaged through improper handling, carelessness or reckless use.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.

MOTOROLA SOLUTIONS







CHARLES TOWN, CITY OF

10/02/2026

The design, technical, pricing, and other information ("Information") furnished with this submission is confidential proprietary information of Motorola Solutions, Inc. or the Motorola Solutions entity providing this quote ("Motorola") and is submitted with the restriction that it is to be used for evaluation purposes only. To the fullest extent allowed by applicable law, the Information is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the Information without the express written permission of Motorola.
MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarl the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved.

10/02/2026

Dear Chief Chris Kutcher,

Motorola Solutions is pleased to present CHARLES TOWN, CITY OF with this quote for quality communications equipment and services. The development of this quote provided us the opportunity to evaluate your requirements and propose a solution to best fulfill your communications needs.

This information is provided to assist you in your evaluation process. Our goal is to provide CHARLES TOWN, CITY OF with the best products and services available in the communications industry. Please direct any questions to Alexander Tirado at Alexander.Tirado@motorolasolutions.com.

We thank you for the opportunity to provide you with premier communications and look forward to your review and feedback regarding this quote.

Sincerely,

Alexander Tirado

Quote Date:10/02/2026
Expiration Date:12/01/2026
Quote Created By:
Alexander Tirado
Alexander.Tirado@
motorolasolutions.com

End Customer:
CHARLES TOWN, CITY OF
Chief Chris Kutcher
ckutcher@charlestownwv.us

Payment Terms:30 NET

Summary:

Any sales transaction resulting from Motorola's quote is based on and subject to the applicable Motorola Standard Terms and Conditions, notwithstanding terms and conditions on purchase orders or other Customer ordering documents. Motorola Standard Terms and Conditions are found at www.motorolasolutions.com/product-terms.

Line #	Item Number	Description	Qty	List Price	Sale Price	Ext. Sale Price
1	PSV00S05486A	MOBILE VIDEO ONSITE CLOUD DEPLOYMENT	1	$8,999.00	$5,000.00	$5,000.00

Grand Total $5,000.00(USD)

Notes:

- Unless otherwise noted, this quote excludes sales tax or other applicable taxes (such as Goods and Services Tax, sales tax, Value Added Tax and other taxes of a similar nature). Any tax the customer is subject to will be added to invoices.

Any sales transaction following Motorola's quote is based on and subject to the terms and conditions of the valid and executed written contract between Customer and Motorola (the ""Underlying Agreement"") that authorizes Customer to purchase equipment and/or services or license software (collectively ""Products""). If no Underlying Agreement exists between Motorola and Customer, then Motorola's Standard Terms of Use and Motorola's Standard Terms and Conditions of Sales and Supply shall govern the purchase of the Products.
Motorola Solutions, Inc.: 500 West Monroe, United States - 60661 ~ #: 36-1115800

Axon Enterprise, Inc.
17800 N 85th St, Scottsdale, Arizona 85255, United States
VAT: 86-0741227
Domestic: (800) 978-2737 | International: +1 800.978.2737

Q-917596-001 Acct: 109431

Issued	**Sep 24, 2026**
Expires	**N/A**
Payment Terms	**N30**
Mode of Delivery	**AUTO-GND**

Charles Town Police Department - WV

Currency: USD

CUSTOMER DETAILS

SHIP TO
Charles Town Police Department - WV
661 South George Street, Suite 100
Charles Town, WV
25414
USA

BILL TO
Charles Town Police Department - WV
661 South George Street, Suite 100
Charles Town, WV
25414
USA

SALES REPRESENTATIVE
David Zador
Email: dzador@axon.com

PRIMARY CONTACT
Chris Kutcher
Phone: (304) 725-2714
Email: ckutcher@charlestownwv.us

QUOTE SUMMARY

Program Length	**60 Months**
Contract Start	**Mar 1, 2027**
Contract End	**Feb 29, 2032**
TOTAL CONTRACT	
Net Total	**$272,706.00**
Est. Tax	**$0.00**
Total Contract Value	**$272,706.00**

DISCOUNT SUMMARY

MSRP	**$414,021.06**
Total Savings	**$141,315.06**

PAYMENT SUMMARY

DATE	SUBTOTAL	EST. TAX	TOTAL
Feb 1, 2027	$54,541.20	$0.00	**$54,541.20**
Feb 1, 2028	$54,541.20	$0.00	**$54,541.20**
Feb 1, 2029	$54,541.20	$0.00	**$54,541.20**
Feb 1, 2030	$54,541.20	$0.00	**$54,541.20**
Feb 1, 2031	$54,541.20	$0.00	**$54,541.20**
Total	**$272,706.00**	**$0.00**	**$272,706.00**

DRAFT

SUMMARY PRICING FOR TERM

ITEM	DESCRIPTION	QTY	TERM (START)	UNBUNDLED	LIST PRICE	NET PRICE	SUBTOTAL	EST. TAX	TOTAL
BODY WORN CAMERA									
B00102	Axon Body Camera Starter Plan	19	60 (3/2027)	**$113.94**	**$59.58**	**$59.58**	**$67,921.20**	$0.00	**$67,921.20**
						Body Worn Camera Total	**$67,921.20**	**$0.00**	**$67,921.20**
DIGITAL EVIDENCE MANAGEMENT									
85760	Axon Auto-Transcribe - Unlimited Service	19	60 (3/2027)	—	**$27.12**	**$0.00**	**$0.00**	$0.00	**$0.00**
73478	Axon Evidence - Redaction Assistant User License	19	60 (3/2027)	—	**$10.85**	**$0.00**	**$0.00**	$0.00	**$0.00**
						Digital Evidence Management Total	**$0.00**	**$0.00**	**$0.00**
FLEET									
Fleet3B	Fleet 3 Basic	22	60 (3/2027)	**$182.46**	**$166.82**	**$155.14**	**$204,784.80**	$0.00	**$204,784.80**
						Fleet Total	**$204,784.80**	**$0.00**	**$204,784.80**
							SUBTOTAL	EST. TAX	TOTAL
	Total						**$272,706.00**	**$0.00**	**$272,706.00**

DRAFT

DELIVERY SCHEDULE

ESTIMATED SHIPPING DATE: Feb 1, 2027

Shipping Location: **661 South George Street, Suite 100, Charles Town, WV, 25414, USA**

HARDWARE		QTY
71019	Axon Body - Dock Powercord - North America	3
70033	Axon Body - Dock Wall Mount - Bracket Assembly	3
11508	Axon Body - Mount - Rapidlock Double MOLLE	21
100466	Axon Body 4 - Cable - USB-C to USB-C	21
100147	Axon Body 4 - Camera - First Responder Black Rapidlock US	20
100206	Axon Body 4 - Dock - Eight-Bay	3
100775	Axon Body 4 - Magnetic Disconnect Cable	21
103346	Axon Fleet - Ericsson R980-5GD-A+5Yr Netcloud	22
101924	Axon Fleet - Taoglas Ant - 7-in-1 4Cell 2WIFI 1GNSS Int	22
72036	Axon Fleet 3 - Standard 2 Camera Kit	22
70112	Axon Signal Vehicle	22
SOFTWARE		**QTY**
CN100147	Axon Body 4 Connected Camera Black US	20
SERVICES		**QTY**
102769	Axon Body - License - Connected Camera 30 Months	20
73391	Axon Fleet 3 - Deployment Per Vehicle - Not Oversized	22
100738	Axon Fleet 3 - SIM Insertion - VZW 4FF	22
WARRANTIES		**QTY**
80464	Axon Body - TAP Warranty - Camera	19
80465	Axon Body - TAP Warranty - Multi-Bay Dock	3
80495	Axon Fleet 3 - Ext Warranty - 2 Camera Kit	22
80379	Axon Signal - Ext Warranty - Signal Vehicle	22

ESTIMATED SHIPPING DATE: Mar 1, 2027

Shipping Location: **661 South George Street, Suite 100, Charles Town, WV, 25414, USA**

SOFTWARE		QTY
85760	Axon Auto-Transcribe - Unlimited Service	19
80400	Axon Evidence - Fleet Vehicle License	22
73840	Axon Evidence - License - Basic	19
73746	Axon Evidence - License - Pro	1
73478	Axon Evidence - Redaction Assistant User License	19
73686	Axon Evidence - Storage - Axon Device Unlimited	19
80410	Axon Evidence - Storage - Fleet 1 Camera Unlimited	44

ESTIMATED SHIPPING DATE: Aug 1, 2029

Shipping Location: **661 South George Street, Suite 100, Charles Town, WV, 25414, USA**

HARDWARE		QTY
73309	Axon Body - TAP Refresh 1 - Camera	19

DRAFT

73689	Axon Body - TAP Refresh 1 - Dock Multi-Bay	3

DRAFT

TERMS & CONDITIONS

This Rough Order of Magnitude estimate is being provided for budgetary and planning purposes only. It is non-binding and is not considered a contractable offer for sale of Axon goods or services.

Tax is estimated based on rates applicable at date of quote and subject to change at time of invoicing. If a tax exemption certificate should be applied, please submit prior to invoicing.

EXCEPTIONS TO STANDARD TERMS AND CONDITIONS

Rewrite Estimates

Estimated Amounts and Contract Terminations. Any amounts stated as due under existing or terminated contracts — including contract transfer balances carried forward to new or pending contracts — are estimates based on payments received as of the calculation date. These estimates may be adjusted if new contracts are not executed on the anticipated dates or if expected payments are not made.

Refresh Shipment Timing

Technology Assurance Plan (TAP) Refresh Prior to Renewal. For Customers with expiring agreements that include TAP refresh rights, Axon may, in its discretion, ship refresh hardware under the existing contract while renewal or replacement agreements are in progress. Any such shipments will be deemed made under the terms of the existing contract until the new contract is fully executed, after which any applicable updates, fees, or adjustments will apply.

Shipment Timing

Shipment Variance . Estimated shipment dates are provided for planning purposes only and are not guarantees. Axon may ship hardware before or after the estimated shipment date, and failure to meet an estimated shipment date will not, by itself, constitute a breach, provided Axon uses commercially reasonable efforts to meet estimated shipment dates.

DRAFT

Axon Enterprise, Inc.
17800 N 85th St, Scottsdale, Arizona 85255, United States
VAT: 86-0741227
Domestic: (800) 978-2737 | International: +1 800.978.2737

Q-964558-001 Acct: 109431

Issued	**Oct 13, 2026**
Expires	**N/A**
Payment Terms	**N30**
Mode of Delivery	**AUTO-GND**

Charles Town Police Department - WV

Currency: USD

CUSTOMER DETAILS

SHIP TO
Charles Town Police Department - WV
661 South George Street, Suite 100
Charles Town, WV
25414
USA

BILL TO
Charles Town Police Department - WV
661 South George Street, Suite 100
Charles Town, WV
25414
USA

SALES REPRESENTATIVE
David Zador
Email: dzador@axon.com

PRIMARY CONTACT
Chris Kutcher
Phone: (304) 725-2714
Email: ckutcher@charlestownwv.us

QUOTE SUMMARY

Program Length	**60 Months**
Contract Start	**Mar 1, 2027**
Contract End	**Feb 29, 2032**
TOTAL CONTRACT	
Net Total	**$300,557.40**
Est. Tax	**$0.00**
Total Contract Value	**$300,557.40**

DISCOUNT SUMMARY

MSRP	**$382,239.46**
Net Price	**$300,557.40**
Total Savings	**$81,682.06**

PAYMENT SUMMARY

DATE	SUBTOTAL	EST. TAX	TOTAL
Feb 1, 2027	$60,111.48	$0.00	**$60,111.48**
Feb 1, 2028	$60,111.48	$0.00	**$60,111.48**
Feb 1, 2029	$60,111.48	$0.00	**$60,111.48**
Feb 1, 2030	$60,111.48	$0.00	**$60,111.48**
Feb 1, 2031	$60,111.48	$0.00	**$60,111.48**
Total	**$300,557.40**	**$0.00**	**$300,557.40**

DRAFT

SUMMARY PRICING FOR TERM

ITEM	DESCRIPTION	QTY	TERM (START)	UNBUNDLED	LIST PRICE	NET PRICE	SUBTOTAL	EST. TAX	TOTAL
BODY WORN CAMERA									
B00102	Axon Body Camera Starter Plan	19	60 (3/2027)	$61.62	$59.58	$59.58	$67,921.20	$0.00	$67,921.20
						Body Worn Camera Total	$67,921.20	$0.00	$67,921.20
DIGITAL EVIDENCE MANAGEMENT									
85760	Axon Auto-Transcribe - Unlimited Service	19	60 (3/2027)	—	$27.12	$0.00	$0.00	$0.00	$0.00
73478	Axon Evidence - Redaction Assistant User License	19	60 (3/2027)	—	$10.85	$0.00	$0.00	$0.00	$0.00
50249	Axon Local - SSL Certificate	1	60 (3/2027)	—	$1.25	$1.25	$75.00	$0.00	$75.00
80277	Axon Local - Pro License Term	1	60 (3/2027)	—	$44.05	$44.05	$2,643.00	$0.00	$2,643.00
80290	Axon Local - Basic License Term Access	19	60 (3/2027)	—	$16.92	$16.92	$19,288.80	$0.00	$19,288.80
80298	Axon Local - Server Term License	1	60 (3/2027)	—	$47.41	$47.41	$2,844.60	$0.00	$2,844.60
50266	Axon Local - Software Installation and Training	1	—	—	$3,000.00	$3,000.00	$3,000.00	$0.00	$3,000.00
						Digital Evidence Management Total	$27,851.40	$0.00	$27,851.40
FLEET									
Fleet3B	Fleet 3 Basic	22	60 (3/2027)	$182.46	$166.82	$155.14	$204,784.80	$0.00	$204,784.80
						Fleet Total	$204,784.80	$0.00	$204,784.80
							SUBTOTAL	**EST. TAX**	**TOTAL**
	Total						$300,557.40	$0.00	$300,557.40

DRAFT

DELIVERY SCHEDULE

ESTIMATED SHIPPING DATE: Feb 1, 2027

Shipping Location: **661 South George Street, Suite 100, Charles Town, WV, 25414, USA**

HARDWARE		QTY
71019	Axon Body - Dock Powercord - North America	3
70033	Axon Body - Dock Wall Mount - Bracket Assembly	3
11508	Axon Body - Mount - Rapidlock Double MOLLE	21
100466	Axon Body 4 - Cable - USB-C to USB-C	21
100147	Axon Body 4 - Camera - First Responder Black Rapidlock US	19
100206	Axon Body 4 - Dock - Eight-Bay	3
100775	Axon Body 4 - Magnetic Disconnect Cable	21
103346	Axon Fleet - Ericsson R980-5GD-A+5Yr Netcloud	22
101924	Axon Fleet - Taoglas Ant - 7-in-1 4Cell 2WIFI 1GNSS Int	22
72036	Axon Fleet 3 - Standard 2 Camera Kit	22
70112	Axon Signal Vehicle	22
SOFTWARE		**QTY**
CN100147	Axon Body 4 Connected Camera Black US	19
SERVICES		**QTY**
102769	Axon Body - License - Connected Camera 30 Months	19
73391	Axon Fleet 3 - Deployment Per Vehicle - Not Oversized	22
100738	Axon Fleet 3 - SIM Insertion - VZW 4FF	22
50266	Axon Local - Software Installation and Training	1
WARRANTIES		**QTY**
80464	Axon Body - TAP Warranty - Camera	19
80465	Axon Body - TAP Warranty - Multi-Bay Dock	3
80495	Axon Fleet 3 - Ext Warranty - 2 Camera Kit	22
80379	Axon Signal - Ext Warranty - Signal Vehicle	22

ESTIMATED SHIPPING DATE: Mar 1, 2027

Shipping Location: **661 South George Street, Suite 100, Charles Town, WV, 25414, USA**

SOFTWARE		QTY
85760	Axon Auto-Transcribe - Unlimited Service	19
80400	Axon Evidence - Fleet Vehicle License	22
73478	Axon Evidence - Redaction Assistant User License	19
80410	Axon Evidence - Storage - Fleet 1 Camera Unlimited	44
80290	Axon Local - Basic License Term Access	19
80277	Axon Local - Pro License Term	1
80298	Axon Local - Server Term License	1
50249	Axon Local - SSL Certificate	1

ESTIMATED SHIPPING DATE: Aug 1, 2029

DRAFT

Charles Town Police Department - WV **Q-964558-001** Generated Oct 14, 2026

Shipping Location: **661 South George Street, Suite 100, Charles Town, WV, 25414, USA**

HARDWARE		QTY
73309	Axon Body - TAP Refresh 1 - Camera	19
73689	Axon Body - TAP Refresh 1 - Dock Multi-Bay	3

DRAFT

TERMS & CONDITIONS

This Rough Order of Magnitude estimate is being provided for budgetary and planning purposes only. It is non-binding and is not considered a contractable offer for sale of Axon goods or services.

Tax is estimated based on rates applicable at date of quote and subject to change at time of invoicing. If a tax exemption certificate should be applied, please submit prior to invoicing.

EXCEPTIONS TO STANDARD TERMS AND CONDITIONS

Rewrite Estimates

Estimated Amounts and Contract Terminations. Any amounts stated as due under existing or terminated contracts — including contract transfer balances carried forward to new or pending contracts — are estimates based on payments received as of the calculation date. These estimates may be adjusted if new contracts are not executed on the anticipated dates or if expected payments are not made.

Refresh Shipment Timing

Technology Assurance Plan (TAP) Refresh Prior to Renewal. For Customers with expiring agreements that include TAP refresh rights, Axon may, in its discretion, ship refresh hardware under the existing contract while renewal or replacement agreements are in progress. Any such shipments will be deemed made under the terms of the existing contract until the new contract is fully executed, after which any applicable updates, fees, or adjustments will apply.

Shipment Timing

Shipment Variance . Estimated shipment dates are provided for planning purposes only and are not guarantees. Axon may ship hardware before or after the estimated shipment date, and failure to meet an estimated shipment date will not, by itself, constitute a breach, provided Axon uses commercially reasonable efforts to meet estimated shipment dates.

DRAFT

One avoided claim would cover the entire five-year program.

INCLUDED Body cameras for **19** officers · in-car cameras for **22** patrol cars · unlimited storage · Auto-Transcribe and Redaction Assistant free · 2029 refresh

ANNUAL COST	ONE SETTLEMENT	PER OFFICER OR CAR, PER DAY
$54,541.20	**$336,900**	**$3.64**
Same payment every year, 2027 to 2031. $272,706.00 total.	Paid by Graham, N.C. in a single excessive-force case - more than this whole program.[5]	Across all 41 covered units. Cameras, storage, software and installation.

For $54,541.20 a year, 34% below MSRP, every officer and patrol car is on camera - in the same system that already holds the department's Taser records.

Charles Town officers already carry Axon Tasers. This adds cameras to that same system.

The department's **Taser 7**, Axon's current electronic control weapon, already reports every use into **Axon Evidence**, Axon's cloud evidence system. These cameras record into that same account: an expansion of a system the city already has, not a new vendor or a second security review.

One vendor, one review. Taser records and camera video share one account, number 109431.[6]

One record per incident. Taser use, body camera and in-car video are stored together, linked by officer and time.

The Taser can start recording. The system can be set so a Taser event turns on nearby cameras automatically.[6]

Why it pays off

- **Most police contacts are traffic stops**, which is why 75% of this estimate is in-car video.[1]
- **Fewer complaints.** Body cameras cut complaints **16.9%** in the leading meta-analysis, a **4.95 to 1** benefit to cost.[2]
- **New body cameras in 2029**, shipped mid-term inside this price.

Answers for council

- **CJIS, FedRAMP High, SOC 2, ISO/IEC 27001.** Certificates are published at **trust.axon.com**.[3]
- **The department controls the data:** retention, access and audit logs, encrypted in transit and at rest.[3]
- **Records requests covered.** Redaction Assistant and Auto-Transcribe, **$43,285.80** at list, are included at $0.00.

PAYMENT SCHEDULE

PROGRAM YEAR	INVOICE DATE	ANNUAL PAYMENT	EST. VALUE GAINED, CUMULATIVE[4]
Year 1	Feb 1, 2027	$54,541.20	**$67,241.99**
Year 2	Feb 1, 2028	$54,541.20	**$134,483.98**
Year 3	Feb 1, 2029	$54,541.20	**$201,725.97**
Year 4	Feb 1, 2030	$54,541.20	**$268,967.96**
Year 5	Feb 1, 2031	$54,541.20	**$336,209.95**
5-year total	**Est. tax $0.00**	**$272,706.00**	**$336,209.95**

Illustrative net position: **$63,503.95 gained** against $272,706.00 paid, counting body cameras only.[4]

Budgetary estimate. Q-917596-001 (Sep 24, 2026) is marked Non-Binding Budgetary Estimate and Draft: a planning estimate, not a contractable offer; final pricing may change. Figures tie to it: MSRP $414,021.06, net $272,706.00, savings $141,315.06 (34.13%, derived; no percentage is stated). Subtotals Body $67,921.20 + DEM $0.00 + Fleet $204,784.80 equal the net total, so no adjustment is needed. $43,285.80 is the list value of 19 Auto-Transcribe ($27.12) and 19 Redaction Assistant ($10.85) licenses over 60 months. Delivery lists 20 Body 4 cameras for 19 plan users. Per day: $54,541.20 / 41 / 365. No Taser hardware or plate recognition included.

1. BJS, Contacts Between Police and the Public, 2015. 75% = Fleet subtotal / net total.

2. Williams et al., NBER WP 28622 (2021), updating Lum et al. (2020). **Counter-evidence:** no significant effect on use of force (-9.6%, p=. 152); NIJ CrimeSolutions rates body cameras "No Effects" for use of force, assaults on officers and arrests; complaint drops may partly reflect reporting changes. Ratio range 0.95 to 26.51.

3. trust.axon.com, accessed Sep 2026 - Axon's published posture; council should review the certificates and Fleet CJIS memo itself. Video also raises privacy and disclosure questions, and records-request labor stays an agency cost.

4. Illustrative, not a forecast. 4.95 times the body-camera spend only ($13,584.24 a year); Fleet is excluded because the research covers body cameras, so this understates the program. Benefits are society-level, not all city cash: about 27% reaches government budgets (about $18,200 a year here), and the low-end ratio gives about $12,900 a year.

5. 2021 Graham, N.C. settlement, reported by CBS News. Scale reference only, not a prediction; payouts vary widely.

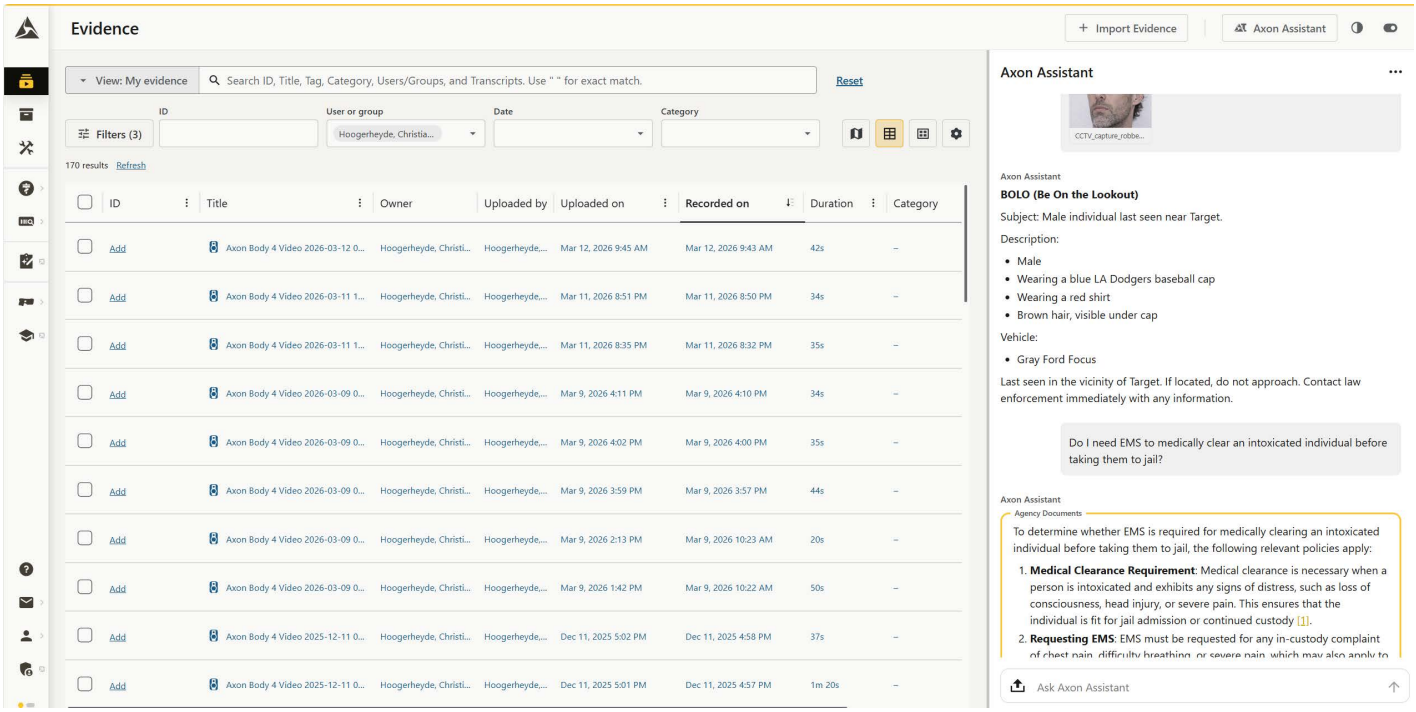
6. axon.com Taser 7 page (docked batteries upload logs to Axon Evidence); Axon Evidence Signal docs (Taser battery events can start body and vehicle cameras). Needs a Signal-capable battery pack, not in this estimate; confirm the department's setup.

Axon Assistant: Secure AI For Public Safety

The CJIS-compliant AI assistant that helps keep agency data protected

Axon Assistant is expanding across the Axon Ecosystem

In 2026, Assistant brings a security and privacy-focused AI workflow for public safety



Evidence.com
Assistant expands to Evidence.com

Axon App
Available on Axon App for iOS and Android

Axon Body Mini
Assistant becomes part of ABW Mini

Axon Body 4 (existing)
Assistant continues on AB4

Privacy and security

- Data securely stored and encrypted within Axon Ecosystem
- Data retained according to customer-configured retention policies
- Secure, compliant, and aligned with Axon's commitment to ethical and responsible AI

Get more from your existing data

Now you can analyze files with Axon Assistant by uploading them from your desktop or mobile phone. Over time you'll also be able to ask questions and deeply analyze other agency data hosted in Axon or other agency systems (such as your CAD system).

What Axon Assistant makes possible in 2026

Assistant will enable agencies to interact across their systems and data more efficiently and automatically glean critical insights from existing data:

- Secure CJIS compliant chat
- Ability to upload and analyze files
- Authentication to access secure info
- Reduced friction between field and back office
    - Your most important data provided in a single view that works across devices
        - Draft a BOLO in Evidence.com; later ask your AB4 for suspect details from the same conversation
        - Upload a photo on desktop; ask follow-up questions from your camera in the field

What Axon Assistant will make possible beyond 2026

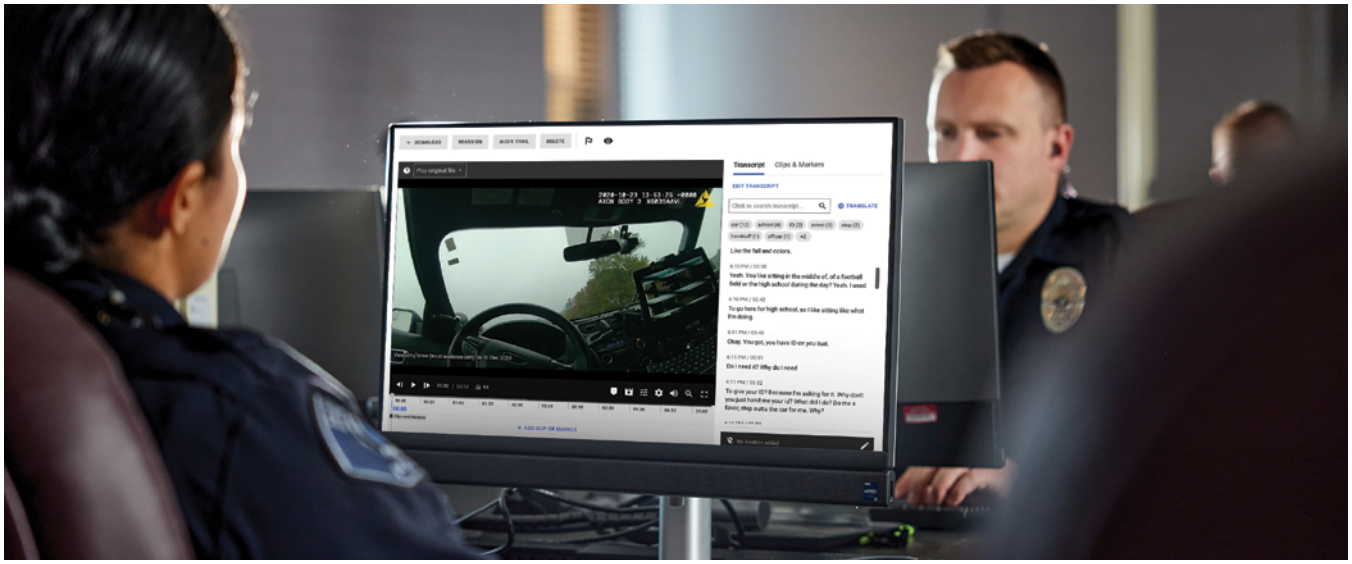
Assistant will expand to more devices within and outside the Axon Ecosystem and more proactively surface deep insights that compound that value of your data:

- Broader reasoning across agency data
- AI that proactively surfaces patterns and insights
- Agency-wide intelligence across internal and third-party sysems
- Deep research capabilities
- Expansion to more Axon solutions
- Extension into 3rd party systems like CAD and RMS

Learn more at axon.com/axon-assistant.

AXON, Axon, Axon Assistant, Axon Ecosystem, Axon Evidence, Axon App and Axon Body 4 are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information visit www.axon.com/legal. All rights reserved. © 2026 Axon Enterprise, Inc.

Auto-Transcribe



Quickly Turn Audio into Easy-to-Search Transcripts

Video and audio evidence are central to every investigation, but the growing volume of digital files demands significant time and resources from law enforcement and justice professionals. Auto-Transcribe helps cut through hours of content by generating AI powered transcripts that provide a reliable starting point to scan, search, and jump to key moments. By making evidence easier to review and navigate, Auto-Transcribe helps you find what matters without needing to watch every minute or listen to every second.

Benefits

Turn Hourse of Evidence Review into Minutes

Time is a valuable resource for agencies balancing high caseloads and administrative demands. While manual review of video and audio files can take hours, Auto-Transcribe accelerates evidence review workflows by generating time-synced transcripts in minutes. These transcripts provide a reliable starting point to scan conversations and jump to key moments, helping reduce time spent on review and support faster, more informed decisions.

Uncover the Moments that Matter

With growing volumes of video and audio evidence, identifying what is relevant can take more time than agencies can afford. Auto-Transcribe helps streamline this process with searchable, time-synced transcripts that make it easier to locate keywords or phrases, even across multiple files. Whether reviewing a single interview or dozens of jail calls, important details can be surfaced faster, helping guide what to review and where to focus.

Re-Imagine Traditional Workflows Powered by Transcription

Auto-Transcribe provides a starting point for more than just evidence review. From report writing with Draft One to streamlined evidence search and audio redaction, fast and dependable transcripts lay the foundation for current and future AI innovations across the Axon ecosystem. By connecting transcripts to high-volume workflows, Auto-Transcribe helps agencies maximize productivity across both investigative and administrative responsibilities.



“We’ve seen a 65 – 75% time savings just by being able to push a button to get a transcript.”

Lieutenant Steve Ferrie,
Rowlett Police Department

Features

Auto-Translate

Generate time-synced translations to easily navigate, understand, and review multilingual evidence. Spanish to English translations are supported now, with additional languages coming in the future.

Fast Evidence Review

Quickly scan time-synced transcripts to identify critical moments in video and audio files. Navigate to specific segments in a video by clicking directly on a word in the transcript.

Transcription Assistant

Easily refine AI-generated transcripts with an intuitive text editor that combines audio, video, and time-synced text to support faster documentation.

Transcript Keyword Search

Search across all transcribed video and audio files within Axon Evidence using a keyword or phrase to locate key moments, without needing to review footage in full.

Auto Redact via Transcript

Redact sensitive audio quickly by muting specific words directly from the transcript. Preserve the integrity of evidence while streamlining the redaction process.

Dictation Assistant

Simplify report writing with voice-to-text capabilities that turn spoken words into written content. Reduce time spent typing while keeping focus on surroundings.

Priority Ranked Video Audit

Review videos automatically recommended based on agency-configured keywords or phrases identified in transcripts. Tailor keywords to prioritize critical moments and gain deeper insights.

Built-In Safeguards

Manage access with permissions, track activity in a digital audit trail, and verify accuracy through approval workflows to help ensure transparency and accountability for all transcripts.

Data Security

Perform evidence reviews and create transcripts on a single platform within the reliable and secure walls of Axon Evidence, built on the Microsoft Azure Government Cloud to uphold the highest levels of data security and CJIS compliance.

All non-Axon products, services, or trademarks are property of their respective owners.

AXON, Axon, Axon Auto-Transcribe, Axon Ecosystem, Axon Evidence and Draft One are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2025 Axon Enterprise, Inc.



AXON FLEET 3
SPOTLIGHT ON RESPOND

IN-CAR MEETS REAL TIME

Every vehicle, any location | Live alerts, maps and streaming

Axon Respond brings real-time situational awareness to your agency's connected devices with features like live maps, alerts, and streaming, transforming your Axon camera hardware from passive evidence recording devices to essential communication tools in the moment. Officers and command staff can get or send help when it's needed, maintain visibility of developing situations, and quickly access and share information as it emerges.

Axon Fleet 3, the next generation in-car video, leverages best-in-class hardware, mobile integrated ALPR, and Respond to help your agency solve crimes and protect your officers and community.

Here are some ways that Respond can be used through Axon Fleet 3 to give your agency more real-time awareness of developing situations. The use cases are endless, so talk to your Axon team about some of the ways you can connect your vehicles to a set of eyes back at the station.

/ TRAFFIC STOP FOLLOWING A PLATE HIT

If an officer receives a plate hit through Axon's ALPR for the vehicle of someone with a criminal history, they can request a live stream while responding to the call for added virtual back-up and visibility.

/ HIGH-SPEED CHASE

If an officer is in pursuit, agency leaders can monitor the vehicle's location on the live map and coordinate a response along the changing route. They can also live stream to stay apprised of the situation and send back-up as needed.

/ STATIONARY LIVE STREAMING FOR EVENTS

If your agency is monitoring a larger event like a race, concert or protest, you can set up vehicles along ingress and egress points and view live streams in the command center.

/ ESCALATION ALERTS

Command staff can receive automatic alerts when abnormal changes are detected. For example, if an officer is responding to a simple Call For Service, but suddenly their vehicle's speed reaches 90mph, an alert could be triggered to notify your command staff that a situation may have changed.

AXON, Axon, are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2022 Axon Enterprise, Inc.

Axon Body 4



Axon Body 4 isn't just a body-worn camera — it's a connected device built to empower real-time policing. With Axon Assistant putting the power of AI right on officers' vests, live communication and streaming for situational awareness, and seamless integration into the Axon Fusus platform, Axon Body 4 gives first responders the tools and information they need to make faster, smarter, safer decisions. All this, in a reliable, durable device with enhanced video performance, smarter controls, and a battery that lasts the whole shift.

Whether you're capturing critical footage or coordinating in real time, Axon Body 4 keeps you connected to your team, your command center, and your community.



Axon Assistant

Axon Assistant is an intuitive AI assistant on the body-worn camera, providing first responders with the information they need, when and where they need it. The push-to-talk interface allows officers to keep their eyes up, instead of down on a phone screen. The first channels of Axon Assistant are Real-Time Translation, automatically translating speech to facilitate communication with community members; General Info, providing officers with answers to common questions they may have in the field and Agency Info, pulling responses from agency-approved sources such as policy, delivering answers to queries directly from the camera via voice.



Capture From Any Angle

More points of view with the POV accessory

You don't have to choose between a body-worn camera and a POV camera — with the optional POV accessory, Axon Body 4 gives you both in the same system for ultimate flexibility. Get the shot from the shoulder, helmet, or around corners using the lightweight, durable accessory. IP67-rated with no charging required, the accessory can be plugged in for use when you need it.

Key Capabilities & Benefits

Communicate and Connect for Safer Responses

With device connectivity enabled, Axon Body 4 enables teams to operate with more confidence and clarity. Real-time alerts and GPS location sharing offer heightened situational awareness, while livestreaming and bidirectional communications allow command staff to gain immediate visibility into critical incidents as they unfold. With included Axon Fusus map access, each connected Axon Body 4 becomes a live node in a broader, smarter network, driving informed responses and safer outcomes.

- **Live locations and alerts:** Know where your officers are and be aware of potential escalations with live locations on the Fusus map and automatic notifications through Axon Signal technology.
- **Livestreaming requests:** Livestreaming gives supervisors real-time visibility to help assess resource needs. Officers can press a button to immediately request livestream support.
- **Bidirectional communications:** Supervisors and support staff can speak directly with officers through the camera's speaker for quick communications.
- **Priority evidence upload:** Upload critical footage automatically for faster review.
- **Real-Time Translation:** Officers can quickly communicate with speakers of 50+ languages during everyday interactions using Axon Assistant, directly accessible on their Axon Body 4. Assistant enables real-time, audible translation through the camera, supporting immediate understanding in the field.
- **Even more confidence in critical moments:** Through our collaboration with AT&T, Axon Body 4 livestreams can get mission-critical priority — the highest level of priority on the FirstNet network — through an optional subscription. This added layer of reliability offers an even more complete picture of the field in major planned and unplanned public safety events such as natural disasters, parades and protests. Axon devices can also appear on FirstNet Fusion for added visibility.

Sharper Video, Longer Battery, Smarter Workflows

Axon Body 4 is designed for full-shift high performance, delivering clear footage, extended battery life, and configurable options that fit the way your agency works.

- **Expanded field of view:** New 160° field of view and 4:3 aspect ratio option increases visibility by 39%.
- **Upgraded sensor:** Enhanced 5 MP resolution brings sharp, clear imagery for every frame.
- **Long-lasting battery:** Large 4300 mAh battery allows for all-day uptime, even with the use of connected features.
- **More storage, kept secure:** 128GB solid-state storage with AES 256-bit encryption for robust security.
- **Quick recharge:** Magnetic, quick-breakaway fast-charge delivers a 20% higher charge in 30 minutes.
- **Flexible configuration:** Programmable buttons, role-based permissions, sleep/mute reminders, and power confirmations are configurable to suit needs.
- **Simple registration:** Register a high volume of cameras — up to 100 at a time — quickly, easily, and at once using the Axon Device Manager and Axon dock.

Key Capabilities & Benefits

One Part of a Connected Ecosystem for More Safety and Efficiency

Seamless integration with other Axon technologies makes Axon Body 4 become an even more powerful source of intelligence, enabling faster response, better collaboration, and more efficiency.

- **Ensure crucial footage is captured:** Axon Signal technology ensures cameras are activated based on configured criteria, like a weapon being pulled from its holster. In the event a camera is never activated during an incident, recover footage from up to 18 hours prior with Video Recall.
- **Leverage other devices for a fuller picture:** Sync body-worn and in-car camera footage from Fleet 3 with multi-cam playback and evidence management workflows.
- **Build a Real-Time Crime Center:** Connect with Axon Fusus for a unified command view of livestreams, GPS locations, and alerts from body-worn cameras as well as other data feeds, all in one platform.
- **Save time writing reports:** With Draft One, use Axon Body 4 footage transcripts to create a first draft of a police report, to spend less time report-writing and more time protecting.

Specifications

Video Resolution	1440, 1080, 720, 480
Video Format	MPEG4
Battery Life	13+ hours
Storage	128 GB
Pre-Event Buffer	Configurable up to 120 seconds
IP Rating	Camera: IP68 | POV accessory: IP67
US Military Standard	MIL-STD-810G
Drop Test	6 feet
Operating Temperature	-4 to 122 fahrenheit
Encryption	XTS-AES-256 full disk encryption

All non-Axon products, services, or trademarks are property of their respective owners.

AXON, Axon, Axon Body 4, Axon Fusus, Axon Assistant, Axon Signal and Axon Fleet 3 are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information visit www.axon.com/legal. All rights reserved. © 2026 Axon Enterprise, Inc.

CaseGuard
AI Redaction & Privacy for All

1700 N Moore Street Suite 1701
Arlington, Virginia 22209

Created Date	10/13/2026
Expiration Date	11/13/2026
Quote Number	19803218

Prepared By	Usman Ahmad
Phone	(703) 932-4069
Email	uahmad@caseguard.com

Bill To Name	Charles Town Police Department
Bill To	661 South George Street Charles Town, West Virginia 25414 United States

Proposed Solution: Ultimate Suite

We are thrilled to partner with your organization to revolutionize your redaction process. To meet your needs, we propose our all-in-one **Ultimate Suite**, a package designed for organizations seeking extraordinary speed, efficiency, and automation for **redacting unlimited multimedia files such as Video/Image, Audio, and Documents**.

- **Each Ultimate license** also includes **48,000 AI Credits for use with AI Audio Redaction** (equivalent to 14,400 minutes of detection) **or AI Document Redaction** (equivalent to 48,000 document analysis).
- **Dedicated Account Manager & live one-on-one training**, in addition to group sessions for the onboarding period.

Product	Sales Price	Quantity	Price Protection	Total
CaseGuard Ultimate Suite	$4,548.00	1.00	1 Year	$4,548.00

Tax	$0.00
Estimated Total	$4,548.00

Overview

CaseGuard is committed to providing the most advanced media editing and redaction solution on the market, tailored to meet the dynamic needs of modern organizations. CaseGuard Studio, our secure, local desktop application, has an intuitive interface, serving thousands of clients from various sectors- including law enforcement, healthcare, education, transportation, finance, and private enterprises- making us confident in our ability to deliver an unparalleled experience.

Unlimited AI Video and Image Redaction

- Automatically detect and redact objects such as **faces, license plates, screens, and notepads** from still or shaky footage recorded using a body-worn cam, dash cam, or handheld cameras and images.
- Unlimited AI detections on videos and images.
- Advanced manual redaction and enhancement tools to ensure precision and complete creative control over your final output.
- Unredact one or more objects (face, license plate, etc.).
- Track and redact any object in your video through “Object Tracking.”
- Video and image editing tools and enhancements (cut, merge, crop).
- Merge videos taken from different cameras/angles into one video “Split Screen.”

AI Audio Redaction with Automatic Transcription and Translation

- Automatically mute or bleep personally identifiable information (PII), such as **names, phone numbers, addresses, SSNs, payment information, and 28 other categories**, from any audio file.
- Includes 48,000 AI Credits for use with AI Audio Redaction, transcription, and translation (equivalent to 14,400 minutes of detection).
- Advanced manual redaction and enhancement tools to ensure precision and complete creative control over your final output.
- Identify and rename speakers.
- Automatically transcribe in over 100 languages and dialects.
- Automatically translate in over 74 languages.
- Provide automatic & manual closed captions.
- Create and apply a custom list of redactions using “List Analysis.”
- Change voice to protect identities.
- Audio editing tools (cut, merge, drop segments of audio).
- Noise removal & change volume.

AI Document Redaction

- Automatically redact personally identifiable information (PII), such as **names, phone numbers, emails, addresses, SSNs, payment information, and more,** from any document, including but not limited to police reports, bank statements, medical documents, and FOIA requests.
- 48,000 AI Credits for AI Document Redaction (equivalent to 48,000 document analysis).
- Find and Redact any word, sentence, or paragraph.
- Search and redact patterns like emails, social security numbers, zip codes, or credit card numbers with one click.
- Create a list of custom patterns, including but not limited to PII, to redact in a document.
- OCR in 10+ languages.
- AI Object Detection for checks, credit cards, and more.
- Create a block list to keep certain words unredacted.
- Anonymize thousands of resumes instantly.
- Edit any document by removing pages, extracting specific pages, merging files, and reordering pages.
- Create and apply a custom watermark.
- Create and save custom redaction templates, then apply them to thousands of similarly formatted documents (e.g., medical forms)
- Implement Bates Stamping.

Additional Features and Benefits:

- High-volume batch processing- redact thousands of files at once using the Bulk Wizard.
- Third-party integrations with **Axon** and **Box**.
- Automatic custom chain of custody reporting, including Standard Report, Exemption Log, Privilege Log, and Analytics Report.
- Team collaboration tools on TeamSpace to support multi-user workflows (reviewing, progress updates, adding assignee, and annotations on files).
- Automated Template Style Redaction via Watcher, which continuously monitors designated cloud storage (S3 buckets) for high-volume, hands-free file processing.
- Dedicated Account Manager & live one-on-one training, in addition to group sessions.
- Workshops for continuous learning for each release.
- Priority support for faster issue resolution.

Client Testimonials

Spokane Police Department
Mike Snell | Police Records

My experience with CaseGuard started in March of 2017. They had been working with my agency since September of 2016, but I didn't come into the mix until March. We had a demonstration provided, and I was blown away. I remember thinking to myself, "This can't *possibly* work that well – this is a demo, of course, they're going to show their software under ideal conditions!". They must have known what I was thinking, because we then used "real world" bodycam videos and we used videos with a variety of light levels, action levels, etc., and the software, while not perfect (nothing ever is), is at least 3-4x better than what I was using previously, for redaction.
For example, I was tasked to do "time trials" – how long it took to redact videos using the "old" method versus CaseGuard. CaseGuard is faster at the actual redacting process, more accurate, easier to use, and uses far fewer keystrokes, 100% of the time. (Now, think about the time saved, which is money saved, as well as "wear and tear" on the employee doing the redactions. 5000 separate keystrokes to redact a video, or 20? Which would you prefer?) Case in point - a video that took me 4 hours to redact using the "old" method, took me an hour and 5 minutes using CaseGuard.
This is just the tip of the iceberg. The folks I have been in contact with are very responsive to requests for assistance, extremely knowledgeable, and friendly; they have and continue to help me numerous times throughout this process. They are also willing to listen to customer ideas about how to make things better with the program.
I truly cannot possibly say enough good things about this product and my experiences with it. I am thrilled with my agency's choice to use CaseGuard, so if you are considering getting imaging software for your agency – please, don't hesitate to give me a call, or send me an email, and I'm happy to tell you my experiences in full detail and answer any "real-world" questions you may have.

Wichita Police Department
Krissie Lagana

The practical and real-life uses of CaseGuard redaction software. I have had the pleasure of using CaseGuard for almost a year now. I found CaseGuard to be a major asset to our Police Department.
Redaction is a necessary tool that goes hand in hand with body-worn videos. I found myself struggling with the daunting task of redacting videos, as my only redaction tool was extremely time-consuming, inaccurate, and not user-friendly.
I began my journey researching what redaction software programs were available and was able to try demos from different companies. This gave me practical experience with different products. My favorite by far was CaseGuard. I found CaseGuard to be user-friendly. I didn't have to learn new terminology to use the system. I was able to quickly navigate through the software and started redacting right away. With CaseGuard, I was able to quickly, efficiently, and accurately redact videos. I used the software to not only redact body camera video, but also surveillance videos.
Through my journey, I found myself using CaseGuard software to benefit the Police Department in ways other than redactions. Ultimately, solving crimes is one of the major functions of the Police Department. I was able to use the enhancement feature built into CaseGuard to assist our detectives in identifying individuals. CaseGuard, along with good detective work, has been able to solve crimes. As a department, we have been able to enhance facial features, tag and vehicle information, and tattoos. This list will continue to grow as the needs of the department present themselves.
The customer service with CaseGuard is above that of any other company. I always get a hold of a knowledgeable staff member who is friendly and willing to go above and beyond to help me with my situation. Many situations I come across are situationally unique, and I need someone who is knowledgeable to help me with my unique situation.
I am very proud to be a customer of CaseGuard. I look forward to growing and expanding with the company as it grows and evolves with body-worn cameras.

Notes
Maintenance, support, and upgrades for CaseGuard Studio are all included. All new features and enhancements will automatically be available

for Ultimate Suite members.

Terms
This proposal is valid for 90 days.

CaseGuard
AI Redaction & Privacy for All

CaseGuard, Inc.
1700 N Moore St Suite 1701
Arlington VA 22209
United States
P: (571) 446-4144 | E: Support@CaseGuard.com

CaseGuard Studio Hardware Recommendations

With any video processing software, the more powerful the machine you use, the faster the results. We usually suggest you try the application on the machines you currently have. If you find them too slow, you should consider investing in more powerful machines and/or components because any program you utilize for this purpose will run slow and be interrupted on the machine used.

Recommended Hardware:

Processor	Intel i5, i7, i9 10th generation or newer. AMD Ryzen 5 5600X or newer.
RAM	16 GB DDR4
Memory Speed	3000 MHz
Memory Capacity	512 GB SSD
Graphics Card	NVIDIA GeForce RTX 2070

The only thing that makes a difference in speed for AI detection is the video graphic card. We recommend having "**Nvidia GeForce RTX 2070**" or higher. However, if your budget does not allow it, CaseGuard supports a wide range of video cards; here is a list of the video cards that CaseGuard was tested on. The performance metrics are based on 3Dmark on the 3DMark Time Spy benchmark.

Advanced Hardware Specifications: (Last modified 8/4/2026 – Performance is subject to change)

Graphics Card	Average Performance	Price (MSRP)
Nvidia GeForce RTX 3060	**8,750**	**$329**
Nvidia GeForce RTX 4060	**10,780**	**$299**
Nvidia GeForce RTX 3060 Ti	**11,710**	**$399**
Nvidia GeForce RTX 5060	**13,100**	**$299**
Nvidia GeForce RTX 3070	**13,231**	**$499**
Nvidia GeForce RTX 4060 Ti	**13,503**	**$399**
Nvidia GeForce RTX 5060 Ti	**14,800**	**$429**
Nvidia GeForce RTX 3080	**17,947**	**$699**
Nvidia GeForce RTX 3090	**19,416**	**$1,499**
Nvidia GeForce RTX 4070 Super	**21,000**	**$599**
Nvidia GeForce RTX 5070	**22,700**	**$549**

Graphics Card	Average Performance	Price (MSRP)
Nvidia GeForce RTX 4070 Ti Super	**24,279**	**$799**
Nvidia GeForce RTX 5070 Ti	**27,821**	**$749**
Nvidia GeForce RTX 4080	**28,173**	**$1,199**
Nvidia GeForce RTX 4080 Super	**28,395**	**$999**
Nvidia GeForce RTX 5080	**32,995**	**$999**
Nvidia GeForce RTX 4090	**36,328**	**$1,599**
Nvidia GeForce RTX 5090	**46,923**	**$1,999**

Estimated Resell Value (Used Market):

The figures below are approximate secondary-market (used) prices as of August 2026 and vary with condition, warranty, and seller. Buying new is generally preferable.

Graphics Card	Est. Resell Price (Used)	Availability / Notes
Nvidia GeForce RTX 3060	**~$260**	Also sold new (~$340)
Nvidia GeForce RTX 4060	—	In production – buy new (~$339)
Nvidia GeForce RTX 3060 Ti	**~$205**	Discontinued
Nvidia GeForce RTX 5060	—	In production – buy new (~$340)
Nvidia GeForce RTX 3070	**~$228**	Discontinued
Nvidia GeForce RTX 4060 Ti	—	In production – buy new (~$424)
Nvidia GeForce RTX 5060 Ti	—	In production – buy new (16 GB ~$525)
Nvidia GeForce RTX 3080	**~$285**	Discontinued
Nvidia GeForce RTX 3090	**~$800**	Discontinued (24 GB)
Nvidia GeForce RTX 4070 Super	**~$549**	Discontinued
Nvidia GeForce RTX 5070	—	In production – buy new (~$599)
Nvidia GeForce RTX 4070 Ti Super	**~$770**	Discontinued
Nvidia GeForce RTX 5070 Ti	—	In production – buy new (~$899)
Nvidia GeForce RTX 4080	**~$1,000**	Discontinued
Nvidia GeForce RTX 4080 Super	**~$856**	Discontinued
Nvidia GeForce RTX 5080	—	In production – buy new (~$1,300)
Nvidia GeForce RTX 4090	**~$3,999**	Discontinued – scarce
Nvidia GeForce RTX 5090	**~$3,999**	In production – scarce (used ≈ new)

Resell values are estimates for general guidance only and are not quotes; used pricing moves week to week. Verify current listings before relying on any figure.

ESTIMATE

Executive Emergency Lighting LLC
21 Southpaw Lane
Shepherdstown, WV 25443

raymuth.eel@gmail.com
+1 (304) 870-4420
emergencylightingllc.com

Bill to
Charles Town Police Department
661 S George St
Charles Town, WV 25414

Estimate details
Estimate no.: 1572
Estimate date: 08/19/2026

Unit: Camera Removal Per Unit

#	Date	Product or service	Description	Qty	Rate	Amount
1.	08/19/2026	**Labor**	Remove Motorola/Watchguard Camera System in customer furnished vehicle. Remove Interior panels to remove all wiring and associated components. Re-install all interior panels. Remove Antenna System	6	$175.00	$1,050.00
2.	08/19/2026	**Shop & Office Fees**	Misc.	1	$170.62	$170.62

Total **$1,220.62**

Accepted date

Accepted by

Criminal Justice Information Services (CJIS) Security Policy

Version 6.0
12/27/2024

Prepared by:
FBI CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Criminal and noncriminal justice agencies need timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 2019. Administered through a shared management philosophy, the CJIS Security Policy (CJISSECPOL) contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the systems that process, store, and transmit Criminal Justice Information (CJI). The Federal Information Security Management Act of 2014 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided to the criminal and noncriminal justice communities.

The essential premise of the CJISSECPOL is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJISSECPOL provides guidance for the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal and noncriminal justice services and information.

The CJISSECPOL integrates presidential directives, federal laws, FBI directives and the criminal and noncriminal justice community decisions along with guidance from the National Crime Prevention and Privacy Compact Council (Compact Council). The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving technology and business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a minimum level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJISSECPOL strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB), and Interface Agencies (IA). Further, as use of criminal history record information (CHRI) for noncriminal justice purposes continues to expand, the CJISSECPOL becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of CHRI.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs, SIBs, and IAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJISSECPOL provides a security framework based on laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
6.0	Policy Modernization Completion	Security Policy Modernization Task Force	12/27/2024	APB & Compact Council

SUMMARY OF CHANGES

Version 6.0

APB Approved Changes

1. **Modernizing the Executive Summary, Section 1: Introduction, Section 2: *CJISSECPOL* Approach, and Section 3: Roles and Responsibilities in the *CJISSECPOL*, Spring 2024, APB#11, SA#2:** update sections with approved changes.

2. **Changing and Refreshing Authenticators in the *CJISSECPOL*, Spring 2024, APB#11, SA#3:** clarifies which authenticator type requires annual changing and clarifies the use of a "banned password" list.

3. **Modernizing System and Services Acquisition (SA) in the *CJISSECPOL*, Spring 2024, APB#11, SA#5:** add definitions and modernize the CJIS Security Policy requirements for:

   System and Services Acquisition Policy and Procedures
   Allocation of Resources
   System Development Lifecycle
   Acquisition Process
   System Documentation
   Security and Privacy Engineering Principles
   External System Services
   Developer Configuration Management
   Developer Testing and Evaluation
   Developer Process, Standards, and Tools

4. **Modernizing Supply Chain and Risk Management (SR) in the *CJISSECPOL*, Spring 2024, APB#11, SA#6:** modernize the CJIS Security Policy requirements for

   Supply Chain Risk Management Policy and Procedures
   Supply Chain Risk Management Plan
   Acquisition Strategies, Tools, and Methods
   Notification Agreements
   Inspection of Systems or Components
   Component Disposal

5. **Modernizing Personnel Security (PS) in the *CJISSECPOL*, Spring 2024, APB#11, SA#7:** modernize the CJIS Security Policy requirements for

   Personnel Security Policy and Procedures
   Position Risk Designation
   Personnel Screening
   Personnel Termination
   Personnel Transfer
   Access Agreements
   External Personnel Security

Personnel Sanctions
Position Descriptions

6. **Modernizing Assessment, Authorization, and Monitoring (CA) in the *CJISSECPOL*, Spring 2024, APB#11, SA#8:** modernize the CJIS Security Policy requirements for

   Assessment, Authorization, and Monitoring Policy and Procedures
   Control Assessments
   Information Exchange
   Plan of Action and Milestones
   Authorization
   Continuous Monitoring
   Internal System Connections

7. **Remove Appendix J and K from the *CJISSECPOL*, Spring 2024, APB#11, SA#9:** remove the indicated appendices.

Administrative Changes

1. There are no Administrative Changes in this version.

Note: Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

KEY TO APB APPROVED CHANGES (e.g., "Section 5.13 Mobile Devices, Fall 2013, APB#11, SA#6, Future CSP for Mobile Devices: add language"):
Section Number and Name
Fall 2013 – Advisory Policy Board cycle and year
APB# – Advisory Policy Board Topic number
SA# – Security and Access Subcommittee Topic number
Topic Paper Title
Summary of change

TABLE OF CONTENTS

Executive Summary ..... **i**
Change Management ..... **ii**
Summary of Changes ..... **iii**
Table of Contents ..... **v**
List of Figures ..... **xv**
List of Priorities ..... **xvi**
1 Introduction **1**
1.1 Purpose 1
1.2 Scope 1
1.3 Relationship to Local Security Policy and Other Policies 1
1.4 Terminology Used in This Document 1
1.5 Distribution of the CJIS Security Policy 2
2 CJIS Security Policy Approach **3**
2.1 CJIS Security Policy Vision Statement 3
2.2 Architecture Independent 3
2.3 Risk Versus Realism 3
3 Roles and Responsibilities **4**
3.1 Shared Management Philosophy 4
3.2 Roles and Responsibilities for Agencies and Parties 4
3.2.1 CJIS Systems Agencies (CSA) 5
3.2.2 CJIS Systems Officer (CSO) 5
3.2.3 Terminal Agency Coordinator (TAC) 6
3.2.4 Criminal Justice Agency (CJA) 6
3.2.5 Noncriminal Justice Agency (NCJA) 6
3.2.6 Contracting Agency (CA) 7
3.2.7 Agency Coordinator (AC) 7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO) 7
3.2.9 Organizational Personnel with Security Responsibilities 8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO) 8
3.2.11 Repository Manager 8
3.2.12 IA Official 9
3.2.13 State Compact Officer (SCO) 9
4 Criminal Justice Information and Personally Identifiable Information **10**
4.1 Criminal Justice Information (CJI) 10
4.1.1 Criminal History Record Information (CHRI) 10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information 11
4.2.1 Proper Access, Use, and Dissemination of CHRI 11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information 11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information 11
4.2.3.1 For Official Purposes 11
4.2.3.2 For Other Authorized Purposes 12
4.2.3.3 CSO Authority in Other Circumstances 12

4.2.4 Storage 12
4.2.5 Justification and Penalties 12
4.2.5.1 Justification 12
4.2.5.2 Penalties 12
4.3 Personally Identifiable Information (PII) 12
5 Policy and Implementation 14
5.1 Policy Area 1: Information Exchange Agreements 15
5.1.1 Information Exchange 15
5.1.2 Monitoring, Review, and Delivery of Services 15
5.1.2.1 Managing Changes to Service Providers 15
ACCESS CONTROL (AC) 16
AC-1 Policy and Procedures 16
AC-2 Account Management 17
(1) Account Management | Automated System Account Management 20
(2) Account Management | Automated Temporary and Emergency Account Management 20
(3) Account Management | Disable Accounts 20
(4) Account Management | Automated Audit Actions 20
(5) Account Management | Inactivity Logout 21
(13) Account Management | Disable Accounts for High-Risk Individuals 21
AC-3 Access Enforcement 21
(14) Access Enforcement | Individual Access 22
AC-4 Information Flow Enforcement 22
AC-5 Separation of Duties 23
AC-6 Least Privilege 24
(1) Least Privilege | Authorize Access to Security Functions 24
(2) Least Privilege | Non-Privileged Access for Nonsecurity Functions 24
(5) Least Privilege | Privileged Accounts 25
(7) Least Privilege | Review of User Privileges 25
(9) Least Privilege | Log Use of Privileged Functions 25
(10) Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions 26
AC-7 Unsuccessful Logon Attempts 26
AC-8 System Use Notification 27
AC-11 Device Lock 28
(1) Device Lock | Pattern-Hiding Displays 28
AC-12 Session Termination 28
AC-14 Permitted Actions without Identification or Authentication 29
AC-17 Remote Access 29
(1) Remote Access | Monitoring and Control 30
(2) Remote Access | Protection of Confidentiality and Integrity Using Encryption 30
(3) Remote Access | Managed Access Control Points 31
(4) Remote Access | Privileged Commands and Access 31
AC-18 Wireless Access 31
(1) Wireless Access | Authentication and Encryption 32
(3) Wireless Access | Disable Wireless Networking 32

AC-19 Access Control for Mobile Devices 32
(5) Access Control for Mobile Devices | Full Device or Container-Based Encryption 33
AC-20 Use of External Systems 33
(1) Use of External Systems | Limits On Authorized Use 34
(2) Use of External Systems | Portable Storage Devices — Restricted Use 35
AC-21 Information Sharing 35
AC-22 Publicly Accessible Content 36
AWARENESS AND TRAINING (AT) 37
AT-1 Policy and Procedures 37
AT-2 Literacy Training and Awareness 38
(2) Literacy Training and Awareness | Insider Threat 39
(3) Literacy Training and Awareness | Social Engineering and Mining 39
AT-3 Role-Based Training 40
(5) Role-Based Training | Processing Personally Identifiable Information 42
AT-4 Training Records 43
AUDIT AND ACCOUNTABILITY (AU) 45
AU-1 Policy and Procedures 45
AU-2 Event Logging 46
AU-3 Content of Audit Records 47
(1) Content of Audit Records | Additional Audit Information 48
(3) Content of Audit Records | Limit Personally Identifiable Information Elements 49
AU-4 Audit Log Storage Capacity 49
AU-5 Response to Audit Logging Process Failures 49
AU-6 Audit Record Review, Analysis, and Reporting 50
(1) Audit Record Review, Analysis, and Reporting | Automated Process Integration 50
(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories 51
AU-7 Audit Record Reduction and Report Generation 51
(1) Audit Record Reduction and Report Generation | Automatic Processing 51
AU-8 Time Stamps 52
AU-9 Protection of Audit Information 52
(4) Protection of Audit Information | Access by Subset of Privileged Users 53
AU-11 Audit Record Retention 53
AU-12 Audit Record Generation 54
ASSESSMENT, AUTHORIZATION, AND MONITORING (CA) 55
CA-1 Policy and Procedures 55
CA-2 Control Assessments 56
(1) Control Assessments | Independent Assessors 57
CA-3 Information Exchange 58
CA-5 Plan of Action and Milestones 61
CA-6 Authorization 61
CA-7 Continuous Monitoring 62
(1) Continuous Monitoring | Independent Assessment 64
(4) Continuous Monitoring | Risk Monitoring 64
CA-9 Internal System Connections 64
CONFIGURATION MANAGEMENT (CM) 66

CM-1 Policy and Procedures 66
CM-2 Baseline Configuration 67
(2) Baseline Configuration | Automation Support for Accuracy and Currency 67
(3) Baseline Configuration | Retention of Previous Configurations 68
(7) Baseline Configuration | Configure Systems and Components for High-Risk Areas ..68
CM-3 Configuration Change Control 69
(2) Configuration Change Control | Testing, Validation, and Documentation of Changes 69
(4) Configuration Change Control | Security and Privacy Representatives 70
CM-4 Impact Analyses 70
(2) Impact Analyses | Verification of Controls 71
CM-5 Access Restrictions for Change 71
CM-6 Configuration Settings 71
CM-7 Least Functionality 72
(1) Least Functionality | Periodic Review 73
(2) Least Functionality | Prevent Program Execution 73
(5) Least Functionality | Authorized Software — Allow-by-Exception 74
CM-8 System Component Inventory 74
(1) System Component Inventory | Updates During Installation and Removal 75
(3) System Component Inventory | Automated Unauthorized Component Detection 76
CM-9 Configuration Management Plan 76
CM-10 Software Usage Restrictions 77
CM-11 User-Installed Software 78
CM-12 Information Location 78
(1) Information Location | Automated Tools to Support Information Location 79
CONTINGENCY PLANNING (CP) 80
CP-1 Policy and Procedures 80
CP-2 Contingency Plan 81
(1) Contingency Plan | Coordinate with Related Plans 82
(3) Contingency Plan | Resume Mission and Business Functions 82
(8) Contingency Plan | Identify Critical Assets 82
CP-3 Contingency Training 83
CP-4 Contingency Plan Testing 84
(1) Contingency Plan Testing | Coordinate with Related Plans 84
CP-6 Alternate Storage Site 84
(1) Alternate Storage Site | Separation from Primary Site 85
(3) Alternate Storage Site | Accessibility 85
CP-7 Alternate Processing Site 86
(1) Alternate Processing Site | Separation from Primary Site 86
(2) Alternate Processing Site | Accessibility 87
(3) Alternate Processing Site | Priority of Service 87
CP-8 Telecommunications Services 87
(1) Telecommunications Services | Priority of Service Provisions 88
(2) Telecommunications Services | Single Points of Failure 88
CP-9 System Backup 89
(1) System Backup | Testing for Reliability and Integrity 89

(8) System Backup | Cryptographic Protection....90
CP-10 System Recovery and Reconstitution....90
(2) System Recovery and Reconstitution | Transaction Recovery....90
IDENTIFICATION AND AUTHENTICATION (IA)....92
IA-0 Use of Originating Agency Identifiers in Transactions and Information Exchanges....92
IA-1 Policy and Procedures....92
IA-2 Identification and Authentication (Organizational Users)....93
(1) Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Privileged Accounts....94
(2) Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts....94
(8) Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant....95
(12) Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials....95
IA-3 Device Identification and Authentication....95
IA-4 Identifier Management....96
(4) Identifier Management | Identify User Status....97
IA-5 Authenticator Management....97
(1) Authenticator Management | Authenticator Types....118
(a) Memorized Secret Authenticators and Verifiers:....118
(b) Look-Up Secret Authenticators and Verifiers....123
(c) Out-of-Band Authenticators and Verifiers....125
(d) OTP Authenticators and Verifiers....130
(e) Cryptographic Authenticators and Verifiers (Including Single- and Multi-Factor Cryptographic Authenticators, Both Hardware- and Software-Based)....134
(2) Authenticator Management | Public Key Based Authentication....137
(6) Authenticator Management | Protection of Authenticators....138
IA-6 Authentication Feedback....138
IA-7 Cryptographic Module Authenticationf....139
IA-8 Identification and Authentication (Non-Organizational Users)....139
(1) Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies....140
(2) Identification and Authentication (Non-Organizational Users) | Acceptance of External Authenticators....140
(4) Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles....140
IA-11 Re-Authentication....141
IA-12 Identity Proofing....141
(2) Identity Proofing | Identity Evidence....141
(3) Identity Proofing | Identity Evidence Validation and Verification....142
(5) Identity Proofing | Address Confirmation....164
INCIDENT RESPONSE (IR)....167
IR-1 Policy and Procedures....167
IR-2 Incident Response Training....168
(3) Incident Response Training | Breach....168

IR-3 Incident Response Testing 169
(2) Incident Response Testing | Coordination with Related Plans 169
IR-4 Incident Handling 169
(1) Incident Handling | Automated Incident Handling Processes 170
IR-5 Incident Monitoring 170
IR-6 Incident Reporting 171
(1) Incident Reporting | Automated Reporting 171
(3) Incident Reporting | Supply Chain Coordination 171
IR-7 Incident Response Assistance 172
(1) Incident Response Assistance | Automation Support for Availability of Information and Supportf 172
IR-8 Incident Response Plan 172
(1) Incident Response Plan | Breaches 173
MAINTENANCE (MA) 175
MA-1 Policy and Procedures 175
MA-2 Controlled Maintenance 176
MA-3 Maintenance Tools 176
(1) Maintenance Tools | Inspect Tools 177
(2) Maintenance Tools | Inspect Media 177
(3) Maintenance Tools | Prevent Unauthorized Removal 177
MA-4 Nonlocal Maintenance 178
MA-5 Maintenance Personnel 178
MA-6 Timely Maintenance 179
MEDIA PROTECTION (MP) 180
MP-1 Policy and Procedures 180
MP-2 Media Access 181
~~MP-3 Media Marking ..... 181~~
MP-4 Media Storage 182
MP-5 Media Transport 183
MP-6 Media Sanitization 183
MP-7 Media Use 184
PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) 186
PE-1 Policy and Procedures 186
PE-2 Physical Access Authorizations 187
PE-3 Physical Access Control 187
PE-4 Access Control for Transmission 188
PE-5 Access Control for Output Devices 188
PE-6 Monitoring Physical Access 189
(1) Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment 189
PE-8 Visitor Access Records 190
(3) Visitor Access Records | Limit Personally Identifiable Information Elements 190
PE-9 Power Equipment and Cabling 190
PE-10 Emergency Shutoff 191
PE-11 Emergency Power 191
PE-12 Emergency Lighting 192
PE-13 Fire Protection 192

(1) Fire Protection | Detection Systems — Automatic Activation and Notification.....193
PE-14 Environmental Controls.....193
PE-15 Water Damage Protection.....193
PE-16 Delivery and Removal.....194
PE-17 Alternate Work Site.....194
PLANNING (PL).....196
PL-1 Policy and Procedures.....196
PL-2 System Security and Privacy Plans.....197
PL-4 Rules of Behavior.....199
(1) Rules of Behavior | Social Media and External Site/Application Usage Restrictions 199
PL-8 Security and Privacy Architectures.....200
PL-9 Central Management.....201
PL-10 Baseline Selection.....202
PL-11 Baseline Tailoring.....202
PERSONNEL SECURITY (PS).....204
PS-1Policy and Procedures.....204
PS-2Position Risk Designation.....205
PS-3Personnel Screening.....205
PS-4Personnel Termination.....207
PS-5Personnel Transfer.....208
PS-6Access Agreements.....209
PS-7External Personnel Security.....209
PS-8Personnel Sanctions.....210
PS-9Position Descriptions.....210
RISK ASSESSMENT (RA).....213
RA-1 Policy and Procedures.....213
RA-2 Security Categorization.....214
RA-3 Risk Assessment.....214
RA-5 Vulnerability Monitoring and Scanning.....215
(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned.....217
(5) Vulnerability Monitoring and Scanning | Privileged Access.....217
(11) Vulnerability Monitoring and Scanning | Public Disclosure Program.....217
RA-7 Risk Response.....218
RA-9 Criticality Analysis.....218
SYSTEM AND SERVICES ACQUISITION (SA).....220
SA-1 Policy and Procedures.....220
SA-2 Allocation of Resources.....221
SA-3 System Development Life Cycle.....221
SA-4 Acquisition Process.....222
(1) Acquisition Process | Functional Properties of Controls.....223
(2) Acquisition Process | Design and Implementation Information for Controls.....224
(9) Acquisition Process | Functions, Ports, Protocols, and Services In Use.....224
(10) Acquisition Process | Use of Approved Piv Products.....225
SA-5 System Documentation.....225
SA-8 Security and Privacy Engineering Principles.....226

(33) Security and Privacy Engineering Principles | Minimization 227
SA-9 External System Services....227
(2) External System Services | Identification of Functions, Ports, Protocols, and Services 230
SA-10 Developer Configuration Management 230
SA-11 Developer Testing and Evaluation 231
SA-15 Development Process, Standards, and Tools....232
(1) Development Process, Standards, and Tools |Criticality Analysis 233
SA-22 Unsupported System Components 234
SYSTEMS AND COMMUNICATIONS PROTECTION (SC) 235
SC-1 Policy and Procedures....235
SC-2 Separation of System and User Functionality....236
SC-4 Information in Shared System Resources....236
SC-5 Denial-of-Service Protection 237
SC-7 Boundary Protection 237
(3) Boundary Protection | Access Points....238
(4) Boundary Protection | External Telecommunications Services 238
(5) Boundary Protection | Deny by Default — Allow by Exception 239
(7) Boundary Protection | Split Tunneling for Remote Devices....239
(8) Boundary Protection | Route Traffic to Authenticated Proxy Servers 240
(24) Boundary Protection | Personally Identifiable Information 240
SC-8 Transmission Confidentiality and Integrity 240
(1) Transmission Confidentiality and Integrity | Cryptographic Protection 241
SC-10 Network Disconnect 242
SC-12 Cryptographic Key Establishment and Management 242
SC-13 Cryptographic Protection....243
SC-15 Collaborative Computing Devices and Applications 243
SC-17 Public Key Infrastructure Certificates 244
SC-18 Mobile Code 244
SC-20 Secure Name/Address Resolution Service (Authoritative Source) 245
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)....245
SC-22 Architecture and Provisioning for Name/Address Resolution Service 246
SC-23 Session Authenticity 246
SC-28 Protection of Information at Rest 246
(1) Protection of Information at Rest | Cryptographic Protection....247
SC-39 Process Isolation 248
SYSTEM AND INFORMATION INTEGRITY (SI) 250
SI-1 Policy and Procedures....250
SI-2 Flaw Remediation 251
(2) Flaw Remediation | Automated Flaw Remediation Status....252
SI-3 Malicious Code Protection....252
SI-4 System Monitoring....253
(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis....255
(4) System Monitoring | Inbound and Outbound Communications Traffic....255
(5) System Monitoring | System-Generated Alerts....255
SI-5 Security Alerts, Advisories, and Directives 256

SI-7 Software, Firmware, and Information Integrity 256
(1) Software, Firmware, and Information Integrity | Integrity Checks 257
(7) Software, Firmware, and Information Integrity | Integration of Detection and Response 257
SI-8 Spam Protection 258
(2) Spam Protection | Automatic Updates 258
SI-10 Information Input Validation 258
SI-11 Error Handling 259
SI-12 Information Management and Retention 259
(1) Information Management and Retention | Limit Personally Identifiable Information Elements 260
(2) Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research 260
(3) Information Management and Retention | Information Disposal 260
SI-16 Memory Protection 261
SUPPLY CHAIN RISK MANAGEMENT (SR) 262
SR-1 Policy and Procedures 262
SR-2 Supply Chain Risk Management Plan 263
(1) Supply Chain Risk Management Plan | Establish SCRM Team 264
SR-5 Acquisition Strategies, Tools, and Methods 264
SR-8 Notification Agreements 265
SR-10 Inspection of Systems or Components 265
SR-12 Component Disposal 266
5.20 Policy Area 20: Mobile Devices 267
5.20.1 Wireless Communications Technologies 267
5.20.1.1 802.11 Wireless Protocols 267
5.20.1.2 Cellular Devices 268
5.20.1.2.1 Cellular Service Abroad 269
5.20.1.2.2 Voice Transmissions Over Cellular Devices 269
5.20.1.3 Bluetooth 269
5.20.1.4 Mobile Hotspots 269
5.20.2 Mobile Device Management (MDM) 270
5.20.3 Wireless Device Risk Mitigations 270
5.20.4 System Integrity 271
5.20.4.1 Patching/Updates 271
5.20.4.2 Malicious Code Protection 271
5.20.4.3 Personal Firewall 271
5.20.5 Incident Response 272
5.20.6 Access Control 272
5.20.7 Identification and Authentication 272
5.20.7.1 Local Device Authentication 272
5.20.7.2 Advanced Authentication 273
5.20.7.2.1 Compensating Controls 273
5.20.7.3 Device Certificates 273
Appendices 274
APPENDIX A: TERMS AND DEFINITIONS A-1

APPENDIX B: ACRONYMS B-1
APPENDIX C: NETWORK TOPOLOGY DIAGRAMS C-1
APPENDIX D: SAMPLE INFORMATION EXCHANGE AGREEMENTS D-1
D.1 CJIS User Agreement D.1-1
D.2 Management Control Agreement D.2-1
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding D.3-1
D.4 Interagency Connection Agreement D.4-1
APPENDIX E: SECURITY FORUMS AND ORGANIZATIONAL ENTITIES E-1
APPENDIX F: SAMPLE FORMS F-1
F.1 Security Incident Response form F.1-1
APPENDIX G: BEST PRACTICES G-1
G.1 Virtualization G.1-1
G.2 Voice over Internet Protocol G.2-1
G.3 Cloud Computing G.3-1
G.4 Mobile Appendix G.4-1
G.5 Administrator Accounts for Least Privilege and Separation of Duties G.5-1
G.6 Encryption G.6-1
G.7 Incident Response G.7-1
G.8 Secure Coding G.8-1
APPENDIX H: SECURITY ADDENDUM H-1
APPENDIX I: REFERENCES I-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components....4
Figure 2 – Dissemination of restricted and non-restricted NCIC data....13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department....15
Figure 4 – Security Awareness Training Use Cases....43
Figure 5 – A Local Police Department's Configuration Management Controls....79
Figure 6 – Digital Identity Model....103
Figure 7 – Notional Strengths of Evidence Types....153
Figure 8 – Types of Identity Evidence Security Features....156
Figure 9 – Validating Identity Evidence....157
Figure 10 – Verification Methods and Strengths....159
Figure 11 – Incident Response Process Initiated by an Incident in a Local Police Department .174
Figure 12 – A Local Police Department's Media Management Policies....185
Figure 13 – Personnel Security Use Cases....211
Figure 14 – System and Communications Protection and Information Integrity Use Cases....248

LIST OF PRIORITIES

NOTE: An asterisk ('*') in the Priority column indicates an existing control from version 5.9.

No.	Control Name	Enhancements	Priority
AC-1	POLICY AND PROCEDURES	AC-1	P2
AC-2	ACCOUNT MANAGEMENT	AC-2 (1) (2) (3) (4) (5) (13)	P1
AC-3	ACCESS ENFORCEMENT	AC-3 (14)	P1*
AC-4	INFORMATION FLOW ENFORCEMENT	AC-4	P1*
AC-5	SEPARATION OF DUTIES	AC-5	P1*
AC-6	LEAST PRIVILEGE	AC-6 (1) (2) (5) (7) (9) (10)	P1*
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-7	P3*
AC-8	SYSTEM USE NOTIFICATION	AC-8	P2*
AC-11	DEVICE LOCK	AC-11 (1)	P4*
AC-12	SESSION TERMINATION	AC-12	P3
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14	P4
AC-17	REMOTE ACCESS	AC-17 (1) (2) (3) (4)	P1
AC-18	WIRELESS ACCESS	AC-18 (1) (3)	P2*
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-19 (5)	P2*
AC-20	USE OF EXTERNAL SYSTEMS	AC-20 (1) (2)	P1
AC-21	INFORMATION SHARING	AC-21	P3*
AC-22	PUBLICLY ACCESSIBLE CONTENT	AC-22	P4
AT-1	POLICY AND PROCEDURES	AT-1	P2
AT-2	LITERACY TRAINING AND AWARENESS	AT-2 (2) (3)	P2*
AT-3	ROLE-BASED TRAINING	AT-3	P2*
AT-3	ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	AT-3 (5)	P2
AT-4	TRAINING RECORDS	AT-4	P4*
AU-1	POLICY AND PROCEDURES	AU-1	P2
AU-2	EVENT LOGGING	AU-2	P2*
AU-3	CONTENT OF AUDIT RECORDS	AU-3 (1)	P2*
AU-3	CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	AU-3 (3)	P2
AU-4	AUDIT LOG STORAGE CAPACITY	AU-4	P2
AU-5	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	AU-5	P2*
AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	AU-6 (1) (3)	P2*
AU-7	AUDIT RECORD REDUCTION AND REPORT GENERATION	AU-7 (1)	P3
AU-8	TIME STAMPS	AU-8	P2*
AU-9	PROTECTION OF AUDIT INFORMATION	AU-9 (4)	P2*
AU-11	AUDIT RECORD RETENTION	AU-11	P4*
AU-12	AUDIT RECORD GENERATION	AU-12	P2
CA-1	POLICY AND PROCEDURES	CA-1	P2
CA-2	CONTROL ASSESSMENTS	CA-2 (1)	P3
CA-3	INFORMATION EXCHANGE	CA-3	P2*
CA-5	PLAN OF ACTION AND MILESTONES	CA-5	P4

No.	Control Name	Enhancements	Priority
CA-6	AUTHORIZATION	CA-6	P3
CA-7	CONTINUOUS MONITORING	CA-7 (1) (4)	P1
CA-9	INTERNAL SYSTEM CONNECTIONS	CA-9	P3
CM-1	POLICY AND PROCEDURES	CM-1	P2
CM-2	BASELINE CONFIGURATION	CM-2 (2) (3) (7)	P1
CM-3	CONFIGURATION CHANGE CONTROL	CM-3 (2) (4)	P2
CM-4	IMPACT ANALYSES	CM-4 (2)	P3
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-5	P1
CM-6	CONFIGURATION SETTINGS	CM-6	P1
CM-7	LEAST FUNCTIONALITY	CM-7 (1) (2) (5)	P1
CM-8	SYSTEM COMPONENT INVENTORY	CM-8 (1) (3)	P1
CM-9	CONFIGURATION MANAGEMENT PLAN	CM-9	P2
CM-10	SOFTWARE USAGE RESTRICTIONS	CM-10	P3
CM-11	USER-INSTALLED SOFTWARE	CM-11	P2
CM-12	INFORMATION LOCATION	CM-12 (1)	P2
CP-1	POLICY AND PROCEDURES	CP-1	P2
CP-2	CONTINGENCY PLAN	CP-2 (1) (3) (8)	P2
CP-3	CONTINGENCY TRAINING	CP-3	P3
CP-4	CONTINGENCY PLAN TESTING	CP-4 (1)	P3
CP-6	ALTERNATE STORAGE SITE	CP-6 (1) (3)	P2
CP-7	ALTERNATE PROCESSING SITE	CP-7 (1) (2) (3)	P2
CP-8	TELECOMMUNICATIONS SERVICES	CP-8 (1) (2)	P2
CP-9	SYSTEM BACKUP	CP-9 (1) (8)	P2
CP-10	SYSTEM RECOVERY AND RECONSTITUTION	CP-10 (2)	P2
IA-1	POLICY AND PROCEDURES	IA-1	P2
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-2 (1) (2) (8) (12)	P1
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	IA-3	P2
IA-4	IDENTIFIER MANAGEMENT	IA-4 (4)	P2*
IA-5	AUTHENTICATOR MANAGEMENT	IA-5 (1) (2) (6)	P1
IA-6	AUTHENTICATION FEEDBACK	IA-6	P3*
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-7	P2
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-8 (1) (2) (4)	P2
IA-11	RE-AUTHENTICATION	IA-11	P2
IA-12	IDENTITY PROOFING	IA-12 (2) (3) (5)	P2
IR-1	POLICY AND PROCEDURES	IR-1	P2*
IR-2	INCIDENT RESPONSE TRAINING	IR-2	P3*
IR-2	INCIDENT RESPONSE TRAINING | BREACH	IR-2 (3)	P3
IR-3	INCIDENT RESPONSE TESTING	IR-3 (2)	P3
IR-4	INCIDENT HANDLING	IR-4 (1)	P2*
IR-5	INCIDENT MONITORING	IR-5	P2*
IR-6	INCIDENT REPORTING	IR-6 (1) (3)	P2*
IR-7	INCIDENT RESPONSE ASSISTANCE	IR-7 (1)	P3*

No.	Control Name	Enhancements	Priority
IR-8	INCIDENT RESPONSE PLAN	IR-8	P2*
IR-8	INCIDENT RESPONSE PLAN | BREACHES	IR-8 (1)	P2
MA-1	POLICY AND PROCEDURES	MA-1	P2
MA-2	CONTROLLED MAINTENANCE	MA-2	P3
MA-3	MAINTENANCE TOOLS	MA-3 (1) (2) (3)	P4
MA-4	NONLOCAL MAINTENANCE	MA-4	P3
MA-5	MAINTENANCE PERSONNEL	MA-5	P3
MA-6	TIMELY MAINTENANCE	MA-6	P3
MP-1	POLICY AND PROCEDURES	MP-1	P2*
MP-2	MEDIA ACCESS	MP-2	P2*
MP-3	MEDIA MARKING	MP-3	P3*
MP-4	MEDIA STORAGE	MP-4	P2*
MP-5	MEDIA TRANSPORT	MP-5	P2*
MP-6	MEDIA SANITIZATION	MP-6	P2*
MP-7	MEDIA USE	MP-7	P2*
PE-1	POLICY AND PROCEDURES	PE-1	P2
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	PE-2	P2*
PE-3	PHYSICAL ACCESS CONTROL	PE-3	P2*
PE-4	ACCESS CONTROL FOR TRANSMISSION	PE-4	P2*
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	PE-5	P3*
PE-6	MONITORING PHYSICAL ACCESS	PE-6 (1)	P2*
PE-8	VISITOR ACCESS RECORDS	PE-8 (3)	P4
PE-9	POWER EQUIPMENT AND CABLING	PE-9	P2
PE-10	EMERGENCY SHUTOFF	PE-10	P2
PE-11	EMERGENCY POWER	PE-11	P2
PE-12	EMERGENCY LIGHTING	PE-12	P2
PE-13	FIRE PROTECTION	PE-13 (1)	P2
PE-14	ENVIRONMENTAL CONTROLS	PE-14	P2
PE-15	WATER DAMAGE PROTECTION	PE-15	P2
PE-16	DELIVERY AND REMOVAL	PE-16	P3
PE-17	ALTERNATE WORK SITE	PE-17	P3*
PL-1	POLICY AND PROCEDURES	PL-1	P2
PL-2	SYSTEM SECURITY AND PRIVACY PLANS	PL-2	P2
PL-4	RULES OF BEHAVIOR	PL-4 (1)	P3
PL-8	SECURITY AND PRIVACY ARCHITECTURES	PL-8	P2
PL-9	CENTRAL MANAGEMENT	PL-9	P4
PL-10	BASELINE SELECTION	PL-10	P3
PL-11	BASELINE TAILORING	PL-11	P3
PS-1	POLICY AND PROCEDURES	PS-1	P2
PS-2	POSITION RISK DESIGNATION	PS-2	P2
PS-3	PERSONNEL SCREENING	PS-3	P2*
PS-4	PERSONNEL TERMINATION	PS-4	P2

No.	Control Name	Enhancements	Priority
PS-5	PERSONNEL TRANSFER	PS-5	P3*
PS-6	ACCESS AGREEMENTS	PS-6	P4
PS-7	EXTERNAL PERSONNEL SECURITY	PS-7	P2*
PS-8	PERSONNEL SANCTIONS	PS-8	P4
PS-9	POSITION DESCRIPTIONS	PS-9	P4
RA-1	POLICY AND PROCEDURES	RA-1	P2
RA-2	SECURITY CATEGORIZATION	RA-2	P2
RA-3	RISK ASSESSMENT	RA-3 (1)	P2
RA-5	VULNERABILITY MONITORING AND SCANNING	RA-5 (2) (5) (11)	P1
RA-7	RISK RESPONSE	RA-7	P2
RA-9	CRITICALITY ANALYSIS	RA-9	P2
SA-1	POLICY AND PROCEDURES	SA-1	P2
SA-2	ALLOCATION OF RESOURCES	SA-2	P2
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3	P2
SA-4	ACQUISITION PROCESS	SA-4 (1) (2) (9) (10)	P2
SA-5	SYSTEM DOCUMENTATION	SA-5	P3
SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	SA-8 (33)	P2
SA-9	EXTERNAL SYSTEM SERVICES	SA-9 (2)	P2
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	SA-10	P2
SA-11	DEVELOPER TESTING AND EVALUATION	SA-11	P2
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	SA-15 (3)	P3
SA-22	UNSUPPORTED SYSTEM COMPONENTS	SA-22	P2
SC-1	POLICY AND PROCEDURES	SC-1	P2
SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY	SC-2	P2*
SC-4	INFORMATION IN SHARED SYSTEM RESOURCES	SC-4	P2*
SC-5	DENIAL-OF-SERVICE PROTECTION	SC-5	P2
SC-7	BOUNDARY PROTECTION	SC-7 (3) (4) (5) (7) (8) (24)	P1
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-8 (1)	P2*
SC-10	NETWORK DISCONNECT	SC-10	P3
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12	P2*
SC-13	CRYPTOGRAPHIC PROTECTION	SC-13	P2*
SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS	SC-15	P2
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17	P2*
SC-18	MOBILE CODE	SC-18	P3
SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	SC-20	P2
SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	SC-21	P2
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	SC-22	P2
SC-23	SESSION AUTHENTICITY	SC-23	P2
SC-28	PROTECTION OF INFORMATION AT REST	SC-28 (1)	P2*
SC-39	PROCESS ISOLATION	SC-39	P2*
SI-1	POLICY AND PROCEDURES	SI-1	P2
SI-2	FLAW REMEDIATION	SI-2 (2)	P1

No.	Control Name	Enhancements	Priority
SI-3	MALICIOUS CODE PROTECTION	SI-3	P1
SI-4	SYSTEM MONITORING	SI-4 (2) (4) (5)	P1
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-5	P2*
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	SI-7 (1) (7)	P1
SI-8	SPAM PROTECTION	SI-8 (2)	P3*
SI-10	INFORMATION INPUT VALIDATION	SI-10	P1
SI-11	ERROR HANDLING	SI-11	P3
SI-12	INFORMATION MANAGEMENT AND RETENTION	SI-12 (1) (2) (3)	P3
SI-16	MEMORY PROTECTION	SI-16	P2
SI-18	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS	SI-18 (4)	P4
SI-19	DE-IDENTIFICATION	SI-19	P4
SR-1	POLICY AND PROCEDURES	SR-1	P2
SR-2	SUPPLY CHAIN RISK MANAGEMENT PLAN	SR-2 (1)	P3
SR-3	SUPPLY CHAIN CONTROLS AND PROCESSES	SR-3	P3
SR-5	ACQUISITION STRATEGIES, TOOLS, AND METHODS	SR-5	P2
SR-6	SUPPLIER ASSESSMENTS AND REVIEWS	SR-6	P2
SR-8	NOTIFICATION AGREEMENTS	SR-8	P3
SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	SR-10	P3
SR-11	COMPONENT AUTHENTICITY	SR-11 (1) (2)	P2
SR-12	COMPONENT DISPOSAL	SR-12	P3

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJISSECPOL provides Criminal Justice Agencies (CJA), Noncriminal Justice Agencies (NCJA), and Interface Agencies (IA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). The essential premise of the CJISSECPOL is to provide the appropriate controls to ensure the continuity of the protection of CJI, from creation through dissemination or destruction, whether at rest or in transit.

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJISSECPOL applies to all entities with access to, or that operate systems which are used to process, store, or transmit CJI. The CJISSECPOL provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CHRI for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJISSECPOL may be used as the sole security policy for the agency. The local agency may complement the CJISSECPOL with a local policy, or the agency may develop their own stand-alone security policy; however, the CJISSECPOL shall always be the minimum standard. State, local, Tribal, territorial (SLTT), and Federal agencies may augment or implement more stringent policies or requirements.

The agency shall develop, disseminate, and maintain formal, documented policy and procedures to facilitate the implementation of the CJISSECPOL and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJISSECPOL areas can be developed for the security program in general, and for a particular information system, when required.

1.4 Terminology Used in This Document

Effective in version 5.9.5, priority and implementation markings have been added to the modernized controls. Based on the FBI Director approved APB recommendation, beginning October 1, 2024, requirements existing prior to the CJISSECPOL modernization (i.e., version 5.9) and those identified as Priority 1 ([Priority 1]) will be the set of sanctionable requirements.

- Non-modernized sections do not have markings but are considered “existing” requirements and continue to be auditable and sanctionable.

- "Existing" modernized requirements and indicated by the [Existing] marking.
- Priority 1 modernized requirements are indicated by the [Priority 1] marking.
- All [Priority 2], [Priority 3], and [Priority 4] modernized requirements fall into a zero-cycle status. The zero-cycle begins October 1, 2024 and ends September 30, 2027.

The following terms are used interchangeably throughout this document:

- Agency and Organization: The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- Organizational Personnel: Individuals belonging to an agency or organization (see above) or contracted to an agency or organization to provide services under contract.
- Information and Data: Both terms refer to CJI.
- System, Information System, Service, or named applications like NCIC: all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- Requirement and Control: These terms refer to a condition or capability that must be met or possessed by a system or system element to satisfy an agreement, standard, specification, or other formally imposed document.

Appendix A and B provide extensive lists of the terms and acronyms.

Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

1.5 Distribution of the CJIS Security Policy

The CJISSECPOL, version 6.0 and later, is a publicly available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJISSECPOL represents the shared responsibility among FBI CJIS, CJIS Systems Agency (CSA), State Identification Bureaus (SIB), and Interface Agency (IA) for the appropriate protection of CJI.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

The CJISSECPOL looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with SLTT and Federal criminal justice agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB, including a representative of the Compact Council, represents criminal and noncriminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJISSECPOL as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

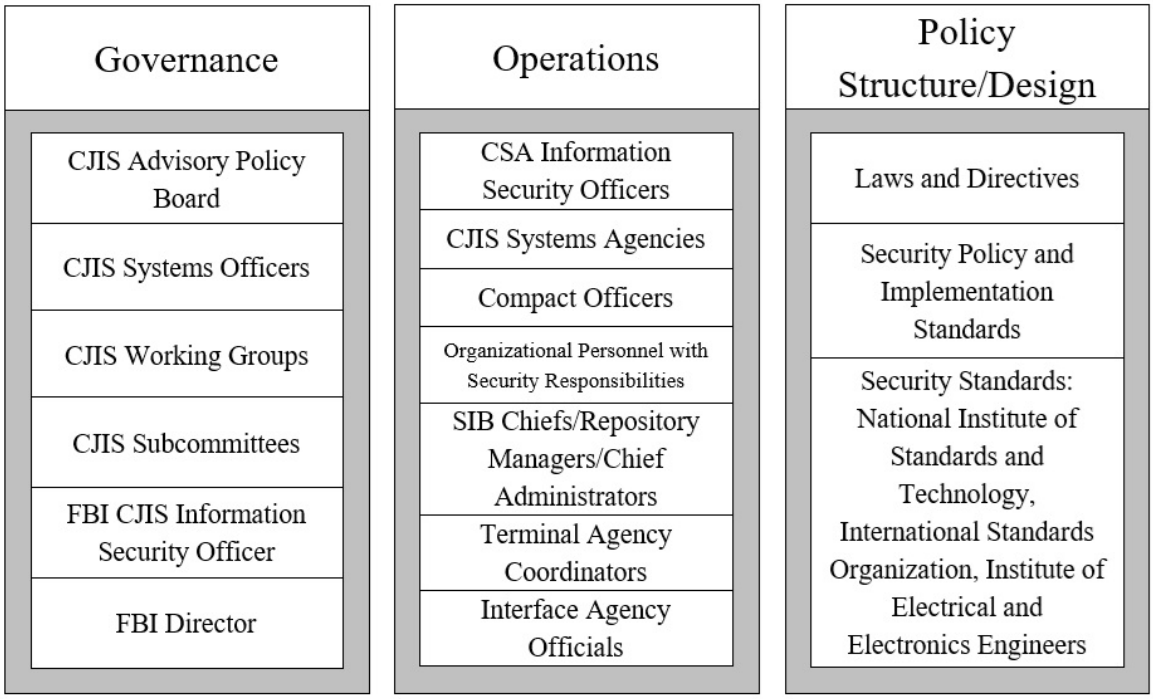


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency (CSA).
2. CJIS Systems Officer (CSO).
3. Terminal Agency Coordinator (TAC).
4. Criminal Justice Agency (CJA).
5. Noncriminal Justice Agency (NCJA).
6. Contracting Agency (CA).
7. Agency Coordinator (AC).
8. CJIS Systems Agency (CSA) Information Security Officer (ISO).
9. Organizational Personnel with Security Responsibilities.
10. FBI CJIS Division Information Security Officer (ISO).
11. SIB Chief/Repository Manager/Chief Administrator.
12. Interface Agency (IA) Official
13. State Compact Officer (SCO).

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent or additional protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority of service required by the law enforcement community, confidentiality, integrity, and availability of CJI.
    a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
    b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.

d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.

e. Ensure each agency having access to CJI has someone designated as the Organizational Personnel with Security Responsibilities.

f. Ensure each Organizational Personnel with Security Responsibilities receives enhanced security awareness training (ref. Awareness and Training (AT)).

g. Approve access to FBI CJIS systems.

h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.

i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.

3. External System Services of Criminal Justice Functions

Responsibility for the management and control of security requirements for information systems which process, store, or transmit CJI shall remain with the CJA. Management and control includes the authority to:

a. Set and enforce standards for the selection, supervision, and termination of access to CJI;

b. Set and enforce policy governing the operation of computers, circuits, and telecommunications terminals,

c. Guarantee the priority service as determined by the CSA.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Agency (CA)

A CA is an agency, whether a CJA, NCJA (public), or NCJA (private), that enters into an agreement with a private contractor subject to the CJIS Security Addendum, The Security and Management Control Outsourcing Standard for Non-Channelers, of the Security and Management Control Outsourcing Standard for Channeling. The CA entering into an agreement with a contractor shall appoint an Agency Coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff as consistent with the NCIC policy.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.

3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Organizational Personnel with Security Responsibilities

Each Organizational Personnel with Security Responsibilities shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e., Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 IA Official

The IA Official is an employee of the IA responsible for planning necessary hardware, software, funding, and training for the IA's authorized access to the CJIS Division's systems. The IA Official shall not be a contract employee.

3.2.13 State Compact Officer (SCO)

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g., within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Threat Screening Center Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Threat Screening Center File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant but did not disclose any information concerning the subject being on the Threat Screening Center File.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Information Exchange Agreements
- Access Control (AC)
- Awareness and Training (AT)
- Auditing and Accountability (AU)
- Assessment, Authorization, and Monitoring (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- Systems and Communications Protection (SC)
- System and Information Integrity (SI)
- Supply Chain Risk Management (SR)
- Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

ACCESS CONTROL (AC)

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing, and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJI.

AC-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to: organizational personnel with access control responsibilities
    1. Agency-level access control policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures; and
c. Review and update the current access control:
    1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures

include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: IA-1, PS-8, SI-12.

AC-2 ACCOUNT MANAGEMENT

[Existing] [Priority 1]

Control:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require conditions for group and role membership;

d. Specify:

   1. Authorized users of the system;
   2. Group and role membership; and
   3. Access authorizations (i.e., privileges) and attributes listed for each account;

Attribute Name
Email Address Text
Employer Name
Federation Id
Given Name
Identity Provider Id
Sur Name
Telephone Number
Identity Provider Id
Unique Subject Id
Counter Terrorism Data Self Search Home Privilege Indicator
Criminal History Data Self Search Home Privilege Indicator
Criminal Intelligence Data Self Search Home Privilege Indicator

Criminal Investigative Data Self Search Home Privilege Indicator

Display Name

Government Data Self Search Home Privilege Indicator

Local Id

NCIC Certification Indicator

N-DEx Privilege Indicator

PCII Certification Indicator

28 CFR Certification Indicator

Employer ORI

Employer Organization General Category Code

Employer State Code

Public Safety Officer Indicator

Sworn Law Enforcement Officer Indicator

Authenticator Assurance Level

Federation Assurance Level

Identity Assurance Level

Intelligence Analyst Indicator

e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with agency policy;
g. Monitor the use of accounts;
h. Notify account managers and system/network administrators within:
    1. One day when accounts are no longer required;
    2. One day when users are terminated or transferred; and
    3. One day when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
    1. A valid access authorization;

2. Intended system usage; and
3. Attributes as listed in AC-2(d)(3);

j. Review accounts for compliance with account management requirements at least annually;

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Discussion: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts. Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, SC-7, SC-12, SC-13.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

[Priority 1]

Control:

Support the management of system accounts using automated mechanisms including email, phone, and text notifications.

Discussion: Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage.

Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Related Controls: None.

(2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

[Priority 1]

Control:

Automatically remove temporary and emergency accounts within 72 hours.

Discussion: Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Related Controls: None.

(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS

[Priority 1]

Control:

Disable accounts within one (1) week when the accounts:

a. Have expired;
b. Are no longer associated with a user or individual;
c. Are in violation of organizational policy; or
d. Have been inactive for 90 calendar days.

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Related Controls: None.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

[Existing] [Priority 1]

Control:

Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion: Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Related Controls: AU-2, AU-6.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

[Priority 1]

Control:

Require that users log out when a work period has been completed.

Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related Controls: AC-11.

(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

[Priority 1]

Control:

Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI.

Discussion: Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Related Controls: AU-6, SI-4.

AC-3 ACCESS ENFORCEMENT

[Existing] [Priority 1]

Control:

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Discussion: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

Related Controls: AC-2, AC-4, AC-5, AC-6, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PS-3, SC-2, SC-4, SC-12, SC-13, SC-28, SI-4, SI-8.

Control Enhancements:

(14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS

[Existing] [Priority 1]

Control:

Provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information.

Discussion: Individual access affords individuals the ability to review personally identifiable information about them held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personally identifiable information is being processed. It can also help individuals ensure that their data is accurate. Access mechanisms can include request forms and application interfaces. For federal agencies, [PRIVACT] processes can be located in systems of record notices and on agency websites. Access to certain types of records may not be appropriate (e.g., for federal agencies, law enforcement records within a system of records may be exempt from disclosure under the [PRIVACT]) or may require certain levels of authentication assurance.

Organizational personnel consult with the senior agency official for privacy and legal counsel to determine appropriate mechanisms and access rights or limitations.

Related Controls: IA-8.

AC-4 INFORMATION FLOW ENFORCEMENT

[Existing] [Priority 1]

Control:

Enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the agency-controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers).

Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk

that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross- domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high- assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Related Controls: AC-3, AC-6, AC-17, AC-19, AC-21, CA-3, CA-9, CM-7, SC-4, SC-7.

AC-5 SEPARATION OF DUTIES

[Existing] [Priority 1]

Control:

a. Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI; and

b. Define system access authorizations to support separation of duties.

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8.

AC-6 LEAST PRIVILEGE

[Existing] [Priority 1]

Control:

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Related Controls: AC-2, AC-3, AC-5, CM-5, CM-11, PL-2, SA-8, SA-15.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

[Existing] [Priority 1]

Control:

Authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:

a. Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and

b. Security-relevant information in hardware, software, and firmware.

Discussion: Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Related Controls: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

[Existing] [Priority 1]

Control:

Require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions.

Discussion: Requiring the use of non-privileged accounts when accessing non-security functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non- privileged account.

Related Controls: AC-17, AC-18, AC-19, PL-4.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

[Existing] [Priority 1]

Control:

Restrict privileged accounts on the system to privileged users.

Discussion: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Related Controls: IA-2, MA-3, MA-4.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

[Existing] [Priority 1]

Control:

a. Review annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges; and

b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

Discussion: The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related Controls: CA-7.

(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS

[Existing] [Priority 1]

Control:

Log the execution of privileged functions.

Discussion: The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a

serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Related Controls: AU-2, AU-3, AU-12.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

[Existing] [Priority 1]

Control:

Prevent non-privileged users from executing privileged functions.

Discussion: Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non- privileged users from executing privileged functions is enforced by AC-3.

Related Controls: None.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

[Existing] [Priority 3]

Control:

a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and

b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Discussion: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks.

In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Related Controls: AC-2, AU-2, AU-6, IA-5.

AC-8 SYSTEM USE NOTIFICATION

[Existing] [Priority 2]

Control:

a. Display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
    1. Users are accessing a restricted information system;
    2. System usage may be monitored, recorded, and subject to audit;
    3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
    4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
    1. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system;
    2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
    3. Include a description of the authorized uses of the system.

Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

Related Controls: AC-14, PL-4, SI-4.

AC-11 DEVICE LOCK

[Existing] [Priority 4]

Control:

a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended.

   NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related Controls: AC-2, AC-7, IA-11, PL-4.

Control Enhancements:

(1) DEVICE LOCK | PATTERN-HIDING DISPLAYS

[Existing] [Priority 4]

Control:

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Discussion: The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Related Controls: None.

AC-12 SESSION TERMINATION

[Priority 3]

Control:

Automatically terminate a user session after a user has been logged out.

Discussion: Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions [i.e., network disconnect]). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related Controls: MA-4, SC-10, SC-23.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

[Priority 4]

Control:

a. Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Discussion: Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be "none."

Related Controls: AC-8, IA-2, PL-2.

AC-17 REMOTE ACCESS

[Existing] [Priority 1]

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Related Controls: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE- 17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Control Enhancements:

(1) REMOTE ACCESS | MONITORING AND CONTROL

[Existing] [Priority 1]

Control:

Employ automated mechanisms to monitor and control remote access methods.

Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-2, AU-6, AU-12.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

[Existing] [Priority 1]

Control:

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Discussion: Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol

that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Related Controls: SC-8, SC-12, SC-13.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

[Existing] [Priority 1]

Control:

Route remote accesses through authorized and managed network access control points.

Discussion: Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

Related Controls: SC-7.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

[Existing] [Priority 1]

Control:

a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs; and
b. Document the rationale for remote access in the security plan for the system.

Discussion: Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Related Controls: AC-6, SC-12, SC-13.

AC-18 WIRELESS ACCESS

[Existing] [Priority 2]

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections.

Discussion: Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SI-4.

Control Enhancements:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

[Existing] [Priority 2]

Control:

Protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption.

Discussion: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: SC-8, SC-12, SC-13.

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

[Existing] [Priority 2]

Control:

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Discussion: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: None.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

[Existing] [Priority 2]

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

Discussion: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations

provide physical or procedural controls to meet the requirements established for protecting information and systems. Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

Related Controls: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SI-3, SI-4.

Control Enhancements:

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION

[Existing] [Priority 2]

Control:

Employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.

Discussion: Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related Controls: SC-12, SC-13, SC-28.

AC-20 USE OF EXTERNAL SYSTEMS

[Existing] [Priority 1]

Control:

a. Establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
    1. Access the system from external systems; and
    2. Process, store, or transmit organization-controlled information using external systems; or
b. Prohibit the use of personally-owned information systems including mobile devices (i.e.,

bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI.

Discussion: External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally-owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations.

Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Control Enhancements:

(1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE

[Priority 1]

Control:

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Discussion: Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls: CA-2.

(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE

[Priority 1]

Control:

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls: MP-7.

AC-21 INFORMATION SHARING

[Existing] [Priority 3]

Control:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and
b. Employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.

Discussion: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may

be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls: AC-3, AC-4, RA-3, SC-15.

AC-22 PUBLICLY ACCESSIBLE CONTENT

[Priority 4]

Control:

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.

Discussion: In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the [PRIVACT] and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

Related Controls: AC-3, AT-2, AT3.

AWARENESS AND TRAINING (AT)

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

AT-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:
    1. Organization-level awareness and training policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;
b. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
c. Review and update the current awareness and training:
    1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made; and
    2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.

Discussion: Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or

role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

AT-2 LITERACY TRAINING AND AWARENESS

[Existing] [Priority 2]

Control:

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
    1. As part of initial training for new users prior to accessing CJI and annually thereafter; and
    2. When required by system changes or within 30 days of any security event for individuals involved in the event;
b. Employ one or more of the following techniques to increase the security and privacy awareness of system users:
    1. Displaying posters
    2. Offering supplies inscribed with security and privacy reminders
    3. Displaying logon screen messages
    4. Generating email advisories or notices from organizational officials
    5. Conducting awareness events
c. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and
d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Discussion: Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices

from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, PL-4, PS-7, SA-8.

Control Enhancements:

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT

[Existing] [Priority 2]

Control:

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Discussion: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING

[Existing] [Priority 2]

Control:

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion: Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks.

Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

AT-3 ROLE-BASED TRAINING

[Existing] [Priority 2]

Control:

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities:
    - All individuals with unescorted access to a physically secure location;
    - General User: A user, but not a process, who is authorized to use an information system;
    - Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform;
    - Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.

    1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and
    2. When required by system changes.

b. Update role-based training content annually and following audits of the CSA and local agencies; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy;

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training;

d. Incorporate the minimum following topics into the appropriate role-based training content:

    1. All individuals with unescorted access to a physically secure location
        a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties
        b. Reporting Security Events
        c. Incident Response Training
        d. System Use Notification
        e. Physical Access Authorizations
        f. Physical Access Control
        g. Monitoring Physical Access
        h. Visitor Control
        i. Personnel Sanctions
    2. General User: A user, but not a process, who is authorized to use an information system. In addition to AT-3 (d) (1) above, include the following topics:
        a. Criminal Justice Information

b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information
c. Personally Identifiable Information
d. Information Handling
e. Media Storage
f. Media Access
g. Audit Monitoring, Analysis, and Reporting
h. Access Enforcement
i. Least Privilege
j. System Access Control
k. Access Control Criteria
l. System Use Notification
m. Session Lock
n. Personally Owned Information Systems
o. Password
p. Access Control for Display Medium
q. Encryption
r. Malicious Code Protection
s. Spam and Spyware Protection
t. Cellular Devices
u. Mobile Device Management
v. Wireless Device Risk Mitigations
w. Wireless Device Malicious Code Protection
x. Literacy Training and Awareness/Social Engineering and Mining
y. Identification and Authentication (Organizational Users)
z. Media Protection

3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to AT-3 (d) (1) and (2) above, include the following topics:
    a. Access Control
    b. System and Communications Protection and Information Integrity
    c. Patch Management
    d. Data backup and storage—centralized or decentralized approach
    e. Most recent changes to the CJIS Security Policy
4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. In addition to AT-3 (d) (1), (2), and (3) above, include the following topics:
    a. Local Agency Security Officer Role
    b. Authorized Recipient Security Officer Role
    c. Additional state/local/tribal/territorial or federal agency roles and responsibilities
    d. Summary of audit findings from previous state audits of local agencies
    e. Findings from the last FBI CJIS Division audit

Discussion: Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations

and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, PL-4, PS-7, PS-9, SA-3, SA-8, SA-11, SR-5, SR-6, SR-11.

Control Enhancements:

(5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION

[Priority 2]

Control:

Provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion: Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments,

[PRIVACT] statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

AT-4 TRAINING RECORDS

[Existing] [Priority 4]

Control:

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for a minimum of three years.

Discussion: Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies. Retention of records for three (3) years accounts for a triennial audit cycle.

Related Controls: AT-2, AT-3, CP-3, IR-2, SI-12.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Awareness and Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific -awareness training, and required all staff to complete this training upon assignment and every year thereafter. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 – All individuals with unescorted access to a physically secure location
A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the awareness training on all the topics identified in CJISSECPOL AT-3 d 1.

Use Case 3 – General User Awareness and Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CJISSECPOL AT-3 d 1 and 2.

Use Case 4 – General User Awareness and Training
A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are

therefore required to be given the awareness training on all the topics identified in CJISSECPOL AT-3 d 1 and 2.

Use Case 5 – Privileged User Awareness and Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems and are therefore required to be given the awareness training on all the topics identified in CJISSECPOL AT-3 d 1, 2, and 3.

AUDIT AND ACCOUNTABILITY (AU)

AU-1 POLICY AND PROCEDURES

[Existing] [Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with audit and accountability responsibilities:
    1. Agency and system-level audit and accountability policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
c. Review and update the current audit and accountability:
    1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

AU-2 EVENT LOGGING

[Priority 2]

Control:

a. Identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III);

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system:

   All successful and unsuccessful:

   1. System log-on attempts
   2. Attempts to use:
      a. Access permission on a user account, file, directory, or other system resource;
      b. Create permission on a user account, file, directory, or other system resource;
      c. Write permission on a user account, file, directory, or other system resource;
      d. Delete permission on a user account, file, directory, or other system resource;
      e. Change permission on a user account, file, directory, or other system resource.
   3. Attempts to change account passwords
   4. Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)
   5. Attempts for users to:
      a. Access the audit log file;
      b. Modify the audit log file;
      c. Destroy the audit log file.

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging annually.

Discussion: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for

each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization.

Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, IA-3, MA-4, MP-4, PE-3, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

AU-3 CONTENT OF AUDIT RECORDS

[Existing] [Priority 2]

Control:

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion: Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f). Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Related Controls: AU-2, AU-8, AU-12, MA-4, SA-8, SI-7, SI-11.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

[Existing] [Priority 2]

Control:

Generate audit records containing the following additional information:

a. Session, connection, transaction, and activity duration;
b. Source and destination addresses;
c. Object or filename involved; and
d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
e. The III portion of the log shall clearly identify:
    1. The operator
    2. The authorized receiving agency
    3. The requestor
    4. The secondary recipient

Discussion: The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Related Controls: None.

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Priority 2]

Control:

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

Discussion: Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3.

AU-4 AUDIT LOG STORAGE CAPACITY

[Priority 2]

Control:

Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements (AU-11).

Discussion: Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, SI-4.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

[Existing] [Priority 2]

Control:

a. Alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure; and

b. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.

Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization- defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the

audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three.

Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, SI-4, SI-12.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

[Existing] [Priority 2]

Control:

a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;

b. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Discussion: Audit record review, analysis, and reporting covers information security- and privacy- related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Related Controls: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION

[Priority 2]

Control:

Integrate audit record review, analysis, and reporting processes using automated mechanisms.

Discussion: Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES

[Priority 2]

Control:

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Discussion: Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Related Controls: AU-12, IR-4.

AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

[Priority 3]

Control:

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

Discussion: Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

Related Controls: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, CM-5, IA-5, IR-4, SI-4.

Control Enhancements:

(1) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

[Priority 3]

Control:

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in AU-3.

Discussion: Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

AU-8 TIME STAMPS

[Existing] [Priority 2]

Control:

a. Use internal system clocks to generate time stamps for audit records;

b. Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Discussion: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls: AU-3, AU-12.

AU-9 PROTECTION OF AUDIT INFORMATION

[Existing] [Priority 2]

Control:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.

Discussion: Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits

the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Related Controls: AC-3, AC-6, AU-6, AU-11, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

Control Enhancements:

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

[Priority 2]

Control:

Authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.

Discussion: Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related Controls: AC-5.

AU-11 AUDIT RECORD RETENTION

[Existing] [Priority 4]

Control:

Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion: Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action.

Related Controls: AU-2, AU-4, AU-5, AU-6, AU-9, MP-6, RA-5, SI-12.

AU-12 AUDIT RECORD GENERATION

[Priority 2]

Control:

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems generating required audit logs;

b. Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Discussion: Audit records can be generated from many different system components. The event types specified in AU-2c are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Related Controls: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, CM-5, MA-4, MP-4, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

CA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with assessment, authorization, and monitoring policy responsibilities:
   1. An assessment, authorization, and monitoring policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;
b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
c. Review and update the current assessment, authorization, and monitoring:
   1. Policy annually and following changes to the assessment criteria and
   2. Procedures annually and following changes to the assessment criteria.

Discussion: Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of assessment, authorization, and monitoring policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

CA-2 CONTROL ASSESSMENTS

[Priority 3]

Control:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

   1. Controls and control enhancements under assessment;

   2. Assessment procedures to be used to determine control effectiveness; and

   3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation and any controls that have been impacted by evolving threats at least once every three years to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

e. Produce a control assessment report that documents the results of the assessment; and

f. Provide the results of the control assessment report to the individual who executed the CJIS User Agreement or is in contract with the FBI.

Discussion: Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles

and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives (i.e., CJIS Systems Officer [CSO], Interface Agency [IA] Official, or FBI Compact Officer [CO]).

To satisfy assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-2.

Related Controls: AC-20, CA-5, CA-6, CA-7, RA-5, SA-11, SI-3, SI-12, SR-2, SR-3.

Control Enhancements:

(1) CONTROL ASSESSMENTS | INDEPENDENT ASSESSORS

[Priority 3]

Control:

Employ independent assessors or assessment teams to conduct control assessments.

Discussion: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are

sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Related Controls: None.

CA-3 INFORMATION EXCHANGE

[Existing] [Priority 2]

Control:

a. Approve and manage the exchange of information between the agency system and external systems using the following agreements when applicable;
   1. Executed CJIS User Agreements
      a. Each CSA, SIB, or IA shall execute a signed written agreement (see Appendix D.1) with the FBI CJIS Division stating their willingness to demonstrate conformity with the CJISSECPOL before accessing and consuming CJIS systems and services as set forth in the agreement.
      b. The agreement shall include the standards, audit, and sanctions governing utilization of CJIS systems and services.
      c. The FBI CJIS Division is authorized to periodically test the ability to penetrate the FBI's network through the external connection or system upon proper notification of all signatories in the user agreement.
   2. Criminal Justice Agency User Agreements
      a. Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.
      b. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

         i. Audit

         ii. Dissemination

         iii. Hit confirmation

         iv. Logging

v. Quality Assurance (QA)
vi. Screening (Criminal Justice Employment)
vii. Security
viii. Timeliness
ix. Training
x. Use of the system
xi. Validation

3. Agreements for Noncriminal Justice Use of CHRI

A CJA, NCJA (public), or NCJA (private) designated to request civil fingerprint-based background checks, with full consent of the individual to whom the background check is taking place, for noncriminal justice functions, shall be eligible for access to CHRI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. The CJA, NCJA (public), or NCJA (private) receiving access to CHRI shall enter into signed written agreements with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. The written agreement shall specify the policies to which the agency must adhere, which inlcudes all pertinent areas of the CJISSECPOL. Each NCJA that directly access FBI systems shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external connection or system. A CJA, NCJA (public), or NCJA (private) authorized to access CHRI for noncriminal justice functions pursuant to federal law or state statute approved by the U.S. Attorney General (defined by the Compact Council as an Authorized Recipient), cannot make CHRI available to another governmental agency, nongovernmental agency, or private contractor to perform noncriminal justice administrative functions without implementation of one of the following:

a. Security and Management Control Outsourcing Standard for Non-Channelers. Implementation is applicable to noncriminal justice administrative functions that do not require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Examples include making fitness determinations, processing, storing, or destroying documents, and maintaining IT platforms that do not connect to CJIS systems. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.
b. Security and Management Control Outsourcing Standard for Channeling. Implementation is applicable only to Channeling functions performed by an FBI-approved Channeler that require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.
c. Management Control Agreement or Security Addendum (see Appendix H) pursuant to Title 28, C.F.R., Section 20.33 (a) (6) or (7). Although by regulation

implementation of a Management Control Agreement or the Security Addendum is applicable to the administration of criminal justice pursuant to that agreement performed on behalf of CJAs, under very limited circumstances, implementation may also be applicable to CJAs that obtain and use CHRI for noncriminal justice purposes. Implementation for noncriminal justice purposes is only applicable when another governmental agency or private contractor performs both criminal justice and noncriminal justice administrative functions involving access to CHRI on behalf of the CJA. It is important to note that if the servicing governmental agency or private contractor solely performs noncriminal justice administrative functions, then the CJA would be required to implement the Security and Management Control Outsourcing Standard for Non-Channelers.

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreements at least triennially or when responsibilities or signatories change.
d. Secondary Dissemination
    1. Log the dissemination of CHRI when released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s). If CJI does not contain CHRI and is not part of an information exchange agreement, then it does not need to be logged.
    2. Validate the requestor of CJI in conformance with the local policy as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission; or a member of the public receiving CJI via authorized dissemination.

Discussion: System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. An example of an NCJA (public) is a county school board. An example of an NCJA (private) is a local bank.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged. how the information is protected) are described in the respective

security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related Controls: AC-4, AC-20, CA-6, IA-3, IR-4, PL-2, RA-3, SA-9, SC-7, SI-12.

CA-5 PLAN OF ACTION AND MILESTONES

[Priority 4]

Control:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones at least every six (6) months or when new information is available based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Related Controls: CA-2, CA-7, RA-7, SI-2, SI-12.

CA-6 AUTHORIZATION

[Priority 3]

Control:

a. Assign a senior official as the responsible official for the system;
b. Assign the CSO, SIB Chief, or IA Official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

    1. Accepts the use of common controls inherited by the system; and

    2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations at least every three (3) years.

Discussion: Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing

officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems.
Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls: CA-2, CA-3, CA-7, RA-3, SA-10, SI-12.

CA-7 CONTINUOUS MONITORING

[Priority 1]

Control:

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored:
    1. AC-2(g) Account Management
    2. AC-17(1) Remote Access | Monitoring and Control
    3. AT-4(a) Training Records
    4. CM-3(f) Configuration Change Control
    5. CM-6(d) Configuration Settings
    6. CM-11(c) User-Installed Software
    7. IR-5 Incident Monitoring
    8. MA-2(b) Controlled Maintenance
    9. MA-3(a) Maintenance Tool
    10. MA-4(a) Nonlocal Maintenance
    11. PE-3(d) Physical Access Control
    12. PE-6 Monitoring Physical Access
    13. PE-14(b) Environmental Controls

14. PE-16 Delivery and Removal
15. PS-7(e) External Personnel Security
16. SA-9(c) External System Services
17. SC-7(a) Boundary Protection
18. SC-7(24)(b) Boundary Protection | Personally Identifiable Information
19. SC-18(b) Mobile Code
20. SI-4 System Monitoring

b. Establishing an ongoing frequency for monitoring and an ongoing frequency for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to organizational personnel with information security, privacy responsibilities, and system/network administrators annually, when security events/incidents occur, and when requested.

Discussion: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements.

Related Controls: AC-2, AC-6, AC-17, AT-4, AU-6, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PL-2, PS-7, RA-3, RA-5, RA-7, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SI-3, SI-4, SI-12, SR-6.

Control Enhancements:

(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

[Priority 1]

Control:

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Discussion: Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Related Controls: None.

(4) CONTINUOUS MONITORING | RISK MONITORING

[Priority 1]

Control:

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring;
b. Compliance monitoring; and
c. Change monitoring.

Discussion: Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Related Controls: None.

CA-9 INTERNAL SYSTEM CONNECTIONS

[Priority 3]

Control:

a. Authorize internal connections of components with the capability to process, store, or transmit CJI to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy

requirements, and the nature of the information communicated;

c. Terminate internal system connections when no longer required or authorized; and

d. Review at least annually the continued need for each internal connection.

Discussion: Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Related Controls: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

CONFIGURATION MANAGEMENT (CM)

CM-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with configuration management responsibilities:
   1. Agency-level configuration management policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
c. Review and update the current configuration management:
   1. Policy annually and following any hardware or software changes to systems which process, store, or transmit CJI; and
   2. Procedures annually and following any hardware or software changes to systems which process, store, or transmit CJI.

Discussion: Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

CM-2 BASELINE CONFIGURATION

[Existing] [Priority 1]

Control:

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system;
b. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services; and
c. Review and update the baseline configuration and topological drawing of the system:
    1. At least annually;
    2. When required due to security-relevant changes to the system and/or security incidents occur; and
    3. When system components are installed or upgraded.

Discussion: Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture. See Appendix C for sample topological/network diagrams.

Related Controls: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, MA-2, PL-8, SA-8, SA-10, SA-15, SC-18.

Control Enhancements:

(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

[Priority 1]

Control:

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms such as configuration management tools, hardware, software, firmware inventory tools, and network management tools.

Discussion: Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the

organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls: CM-7, IA-3, RA-5.

(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

[Priority 1]

Control:

Retain at least one (1) previous version of baseline configurations of the system to support rollback.

Discussion: Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Related Controls: None.

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS

[Existing] [Priority 1]

Control:

a. Issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk; and

b. Apply the following controls to the systems or components when the individuals return from travel: examine the device for signs of physical tampering, purge and reimage disk drives and/or devices as required, and ensure all security controls are in place and functional.

Discussion: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

Related Controls: MP-4, MP-5.

CM-3 CONFIGURATION CHANGE CONTROL

[Priority 2]

Control:

a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for two (2) years;
f. Monitor and review activities associated with configuration-controlled changes to the system; and
g. Coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates, upgrades, replacements, etc.) to the information system are required.

Discussion: Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, SA-8, SA-10, SC-28, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Control Enhancements:

(2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

[Priority 2]

Control:

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Discussion: Changes to systems include modifications to hardware, software, or firmware

components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Related Controls: None.

(4) CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES

[Priority 2]

Control:

Require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board.

Discussion: Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3g.

CM-4 IMPACT ANALYSES

[Priority 3]

Control:

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Discussion: Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses

also include risk assessments to understand the impact of the changes and determine if additional controls are required.

Related Controls: CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, SA-5, SA-8, SA-10, SI-2.

Control Enhancements:

(2) IMPACT ANALYSES | VERIFICATION OF CONTROLS

[Priority 3]

Control:

After-system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Discussion: Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Related Controls: SA-11.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

[Existing] [Priority 1]

Control:

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Discussion: Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

Related Controls: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SI-2, SI-10.

CM-6 CONFIGURATION SETTINGS

[Priority 1]

Control:

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards;

b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI based on operational requirements; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline [USGCB] and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SI-2, SI-4.

CM-7 LEAST FUNCTIONALITY

[Existing] [Priority 1]

Control:

a. Configure the system to provide only essential capabilities to meet operational requirements; and

b. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services which are not required.

Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA- 8 and SC-2).

Related Controls: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC- 2, SC-7, SI-4.

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

[Existing] [Priority 1]

Control:

a. Review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

b. Disable or remove functions, ports, protocols, software, and/or services within the system deemed to be unnecessary and/or unsecure.

Discussion: Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related Controls: AC-18.

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

[Priority 1]

Control:

Prevent program execution in accordance with rules of behavior and/or rules authorizing the

terms and conditions of software program usage.

Discussion: Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

Related Controls: CM-8, PL-4, PS-6.

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION

[Priority 1]

Control:

a. Identify software programs authorized to execute on the system;

b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

c. Review and update the list of authorized software programs annually.

Discussion: Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in SC-7.

Related Controls: CM-2, CM-6, CM-8, CM-10, SA-10, SI-7.

CM-8 SYSTEM COMPONENT INVENTORY

[Priority 1]

Control:

a. Develop and document an inventory of system components that:

   1. Accurately reflects the system;

   2. Includes all components within the system;

   3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location; and

b. Review and update the system component inventory annually.

Discussion: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces.

Related Controls: CM-2, CM-7, CM-9, CM-10, CM-11, CP-2, CP-9, MA-2, MA-6, SA-4, SA-5, SI-2.

Control Enhancements:

(1) SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL

[Priority 1]

Control:

Update the inventory of system components as part of component installations, removals, ans system updates.

Discussion: Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and

documented. System updates include hardware, software, and firmware components.

Related Controls: None.

(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

[Priority 1]

Control:

a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly; and
b. Take the following actions when unauthorized components are detected: disable or isolate the unauthorized components and notify organizational personnel with security responsibilities.

Discussion: Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components. Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as "sandboxing."

Related Controls: AC-19, CA-7, RA-5, SC-3, SC-39, SI-3, SI-4, SI-7.

CM-9 CONFIGURATION MANAGEMENT PLAN

[Priority 2]

Control:

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the system and places the configuration items under configuration management;
d. Is reviewed and approved by organizational personnel with information security responsibilities and organizational personnel with configuration management responsibilities; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

Discussion: Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, SA-10, SI-12.

CM-10 SOFTWARE USAGE RESTRICTIONS

[Priority 3]

Control:

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Discussion: Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Related Controls: AC-17, AU-6, CM-7, CM-8, SC-7.

CM-11 USER-INSTALLED SOFTWARE

[Priority 2]

Control:

a. Establish agency-level policies governing the installation of software by users;

b. Enforce software installation policies through automated methods; and

c. Monitor policy compliance through automated methods at least weekly.

Discussion: If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Related Controls: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

CM-12 INFORMATION LOCATION

[Priority 2]

Control:

a. Identify and document the location of CJI and the specific system components on which the information is processed, stored, or transmitted;
b. Identify and document the users who have access to the system and system components where the information is processed and stored; and
c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Discussion: Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood, and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides. The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8).

Related Controls: AC-2, AC-3, AC-4, AC-6, CM-8, RA-2, SA-4, SA-8, SC-4, SC-28, SI-4, SI-7.

Control Enhancements:

(1) INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION

[Priority 2]

Control:

Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy.

Discussion: The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

Related Controls: None.

Figure 5 – A Local Police Department's Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

CONTINGENCY PLANNING (CP)

CP-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with contingency planning responsibilities:
    1. Agency-level contingency planning policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;
b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and
c. Review and update the current contingency planning:
    1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises; and
    2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.

Discussion: Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies,

standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

CP-2 CONTINGENCY PLAN

[Priority 2]

Control:

a. Develop a contingency plan for the system that:
    1. Identifies essential mission and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
    5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
    6. Addresses the sharing of contingency information; and
    7. Is reviewed and approved by agency head or their designee;
b. Distribute copies of the contingency plan to organizational personnel with contingency planning or incident response duties;
c. Coordinate contingency planning activities with incident handling activities;
d. Review the contingency plan for the system annually;
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to organizational personnel with contingency planning or incident response duties;
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.

Discussion: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience.

Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Related Controls: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-6, IR-8, MA-6, MP-2, MP-4, MP-5, PL-2, SA-15, SC-7, SC-23, SI-12.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

[Priority 2]

Control:

Coordinate contingency plan development with organizational elements responsible for related plans.

Discussion: Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

Related Controls: None.

(3) CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS

[Priority 2]

Control:

Plan for the resumption of essential mission and business functions within twenty-four (24) hours of contingency plan activation.

Discussion: Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Related Controls: None.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

[Priority 2]

Control:

Identify critical system assets supporting essential mission and business functions.

Discussion: Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets.

Related Controls: CM-8, RA-9.

CP-3 CONTINGENCY TRAINING

[Priority 3]

Control:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:
    1. Within thirty (30) days of assuming a contingency role or responsibility;
    2. When required by system changes; and
    3. Annually thereafter; and
b. Review and update contingency training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.

Discussion: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including

lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related Controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4.

CP-4 CONTINGENCY PLAN TESTING

[Priority 3]

Control:

a. Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises.
b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed.

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, SR-2.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

[Priority 3]

Control:

Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion: Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Related Controls: IR-8.

CP-6 ALTERNATE STORAGE SITE

[Priority 2]

Control:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

[Priority 2]

Control:

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

[Priority 2]

Control:

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational

assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls: RA-3.

CP-7 ALTERNATE PROCESSING SITE

[Priority 2]

Control:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of operations for essential mission and business functions within the time period defined in the system contingency plan(s) when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Discussion: Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

[Priority 2]

Control:

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

[Priority 2]

Control:

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related Controls: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

[Priority 2]

Control:

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Discussion: Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Related Controls: None.

CP-8 TELECOMMUNICATIONS SERVICES

[Priority 2]

Control:

Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within the time period as defined in the system contingency plan(s) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Discussion: Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8. Alternate telecommunications services reflect

the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls: CP-2, CP-6, CP-7, SC-7.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

[Priority 2]

Control:

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
b. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Discussion: Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

Related Controls: None.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

[Priority 2]

Control:

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Discussion: In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is

important to have provider transparency for the actual physical transmission capability for telecommunication services.

Related Controls: None.

CP-9 SYSTEM BACKUP

[Priority 2]

Control:

a. Conduct backups of user-level information contained in operational systems for essential business functions as required by the contingency plans;

b. Conduct backups of system-level information contained in the system as required by the contingency plans;

c. Conduct backups of system documentation, including security- and privacy-related documentation as required by the contingency plans; and

d. Protect the confidentiality, integrity, and availability of backup information.

Discussion: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-5 and SC-8. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., criminal justice information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4.

Control Enhancements:

(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

[Priority 2]

Control:

Test backup information as required by the contingency plans to verify media reliability and information integrity.

Discussion: Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls: CP-4.

(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION

[Priority 2]

Control:

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI.

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13, SC-28.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

[Priority 2]

Control:

Provide for the recovery and reconstitution of the system to a known state within the timeframe as required by the contingency plans after a disruption, compromise, or failure.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8.

Control Enhancements:

(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

[Priority 2]

Control:

Implement transaction recovery for systems that are transaction-based.

Discussion: Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Related Controls: None.

IDENTIFICATION AND AUTHENTICATION (IA)

Identification is a unique, auditable representation of an identity within an information system usually in the form of a simple character string for each individual user, machine, software component, or any other entity. Authentication refers to mechanisms or processes to verify the identity of a user, process, or device, as a prerequisite to allowing access to a system's resources.

IA-0 USE OF ORIGINATING AGENCY IDENTIFIERS IN TRANSACTIONS AND INFORMATION EXCHANGES

[Existing]

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

NOTE: This control will be included in AC-3 Access Enforcement when modernized.

IA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to authorized personnel:
   1. Agency/Entity identification and authentication policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;
b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:
    1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

DISCUSSION: Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AC-1, PS-8, SI-12.

Control Enhancements: None.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

[Existing] [Priority 1]

Control:

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

DISCUSSION: Organizations can satisfy the identification and authentication requirements by complying with the requirements in [HSPD 12]. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is

obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.

Related Controls: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

[Priority 1]

Control:

Implement multi-factor authentication for access to privileged accounts.

DISCUSSION: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5, AC-6.

(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

[Priority 1]

Control:

Implement multi-factor authentication for access to non-privileged accounts.

DISCUSSION: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know

(e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5.

(8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT

[Priority 1]

Control:

Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

DISCUSSION: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

Related Controls: None.

(12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS

[Priority 1]

Control:

Accept and electronically verify Personal Identity Verification-compliant credentials.

DISCUSSION: Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using [SP 800-79-2]. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in [SP 800-166]. The DOD Common Access Card (CAC) is an example of a PIV credential.

Related Controls: None.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

[Priority 2]

Control:

Uniquely identify and authenticate agency-managed devices before establishing network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset.

DISCUSSION: Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

Related Controls: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-11, SI-4.

IA-4 IDENTIFIER MANAGEMENT

[Existing] [Priority 2]

Control:

Manage system identifiers by:

a. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for one (1) year.

DISCUSSION: Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Related Controls: AC-5, IA-2, IA-3, IA-5, IA-8, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PS-3, PS-4, PS-5.

Control Enhancements:

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

[Priority 2]

Control:

Manage individual identifiers by uniquely identifying each individual as agency or nonagency.

DISCUSSION: Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

Related Controls: None.

IA-5 AUTHENTICATOR MANAGEMENT

[Priority 1]

Control:

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing memorized secret authenticators annually or when there is evidence of authenticator compromise; changing or refreshing all other authenticator types as they expire or when there is evidence of authenticator compromise;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

j. AAL2 Specific Requirements

Control:

All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:

(1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.

SUPPLEMENTAL GUIDANCE: A multi-factor authenticator requires two factors to execute a single authentication event, such as a cryptographically- secure device with an integrated biometric sensor that is required to activate the device. Nine different authenticator types are recognized, representing something you know (a memorized secret), something you have (a physical authenticator), or combinations of physical authenticators with either memorized secrets or biometric modalities (something you are). Multi-factor (MF) authentication is required at AAL2. MF authentication at AAL2 may be performed using the following AAL2 permitted authenticator types: MF OTP Device, MF Crypto Software, or MF Crypto Device; or a memorized secret used in combination with the following permitted single-factor authenticators: Look-Up Secret, Out-of-Band authenticator, SF OTP Device, SF Crypto Software, or SF Crypto Device.

(2) If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator.

SUPPLEMENTAL GUIDANCE: Multifactor authentication requires the use of two different authentication factors. See IA-5 j (1) for permitted authenticator types at AAL2.

(3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography.

SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

(4) At least one authenticator used at AAL2 SHALL be replay resistant.

SUPPLEMENTAL GUIDANCE: Replay resistance is a characteristic of most, although not all, physical authenticators. A given output of the authenticator is required to be accepted for only one authentication transaction. For example, the output of a time-based OTP device or an out-of-band device is considered replay resistant if it can only be used for at most one authentication transaction during its validity period. If it can be used for more than one during this period, it is not replay resistant.

(5) Communication between the claimant and verifier SHALL be via an authenticated protected channel.

SUPPLEMENTAL GUIDANCE: Communication between claimant or user and verifier or agency is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to Man-in-the-Middle (MitM) attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. Mutual authentication of the communication channel is not required unless that is part of the process of authenticating the claimant. Accordingly, the verifier is only responsible the use of an appropriately secure communications protocol.

(6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.

SUPPLEMENTAL GUIDANCE: Verifiers operated by or on behalf of government agencies are required to be validated to meet FIPS 140 requirements. The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software).

(7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.

SUPPLEMENTAL GUIDANCE: The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software). While authenticators are not directly the responsibility of the CSP (particularly in the case of bring- your-own authenticators), the CSP is still responsible for ensuring that a sufficiently strong and FIPS 140 validated authenticator is being used. Binding of CSP-supplied authenticators that are known to meet validation criteria is sufficient.

(8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.

SUPPLEMENTAL GUIDANCE: This requirement applies to multi-factor authenticators resident on a smartphone or similar device; single-factor authenticators on such devices would only provide a single (physical) authentication factor. Unlocking of a device such as a smartphone may be done for any number of reasons unrelated to authentication, and such devices are normally in an unlocked state for a period of time thereafter. Human action such as entry of a memorized secret or presentation of a biometric factor needs to be provided that is directly associated with the authentication event. Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type.

(9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be met.

SUPPLEMENTAL GUIDANCE: Detailed conformance criteria applicable to the use of biometrics are contained in section IA-5 m Biometric Requirements. Since verification of biometric factors is not deterministic due to measurement errors in collection of the

biometric information, evaluation of performance, and, most importantly, false accept rate, is important to ensure security of the authentication process.

(10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.

SUPPLEMENTAL GUIDANCE: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. At AAL2, providing a memorized secret or biometric factor is sufficient for reauthentication prior to the expiration time.

(11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.

SUPPLEMENTAL GUIDANCE: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. At AAL2, providing a memorized secret or biometric factor is sufficient for reauthentication prior to the expiration time.

(12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJISSECPOL.

The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.

SUPPLEMENTAL GUIDANCE: NIST SP 800-53 provides a comprehensive catalog of controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs and risk environments for federal information systems. These controls are the operational, technical, and management safeguards to maintain the integrity, confidentiality, and security of federal information systems and are intended to be used in conjunction with the NIST risk management framework outlined in SP 800-37 and SP 800-63-3 section 5 Digital Identity Risk Management. NIST SP 800-53 presents security control baselines determined by the security categorization of the information system (low, moderate or high) from NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. For IAL2, the moderate baseline controls (see https://nvd.nist.gov/800-53/Rev4/impact/moderate) may be considered the starting point for the selection, enhancement, and tailoring of the security controls presented. Guidance on tailoring the control baselines to best meet the organization's risk environment, systems and operations is presented in SP 800- 53 section 3.2. Tailoring Baseline Security Controls.

While SP 800-53 and other NIST Special Publications in the SP-800-XXX series apply to federal agencies for the implementation of the Federal information Security Management Act (FISMA), non-federal entities providing services for federal information services also are subject to FISMA and should similarly use SP 800-53 and associated publications for appropriate controls. Non-federal entities may be subject to and conformant with other

applicable controls systems and processes for information system security (e.g., FEDRAMP, ISO/IEC 27001). SP-63A allows the application of equivalent controls from such standards and processes to meet conformance with this criterion.

(13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.

SUPPLEMENTAL GUIDANCE: It is recommended that CSPs document any specific retention policies they are subject to, in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.

The CSP is responsible for the proper handling, protection, and retention or disposal of any sensitive data it collects, even after it ceases to provide identity proofing and enrollment services. A CSP may document its policies and procedures for the management of the data is collects in a data handling plan or other document.

(14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.

SUPPLEMENTAL GUIDANCE: This is a conditional requirement and depends on the basis for CSP records retention. Absent clear jurisdictional requirements, risk management processes, including privacy and security risk assessment, need to be performed for records retention decisions. The records retention duration is required to be derived from a risk-based decision process.

k. Privacy requirements that apply to all CSPs, verifiers, and RPs.

(1) The CSP SHALL employ appropriately tailored privacy controls from the CJISSECPOL.

SUPPLEMENTAL GUIDANCE: This requirement establishes overall privacy posture of the CSP.

(2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk.

SUPPLEMENTAL GUIDANCE: Predictability and manageability measures include providing clear notice, obtaining subscriber consent, and enabling selective use or disclosure of attributes. Predictability is meant to build trust and provide accountability and

requires full understanding (and disclosure) of how the attribute information will be used. Manageability also builds trust by demonstrating a CSPs ability to control attribute information throughout processing – collection, maintenance, retention.

l. General requirements applicable to AAL2 authentication process.

(1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.

SUPPLEMENTAL GUIDANCE: Instruction should address aspects of protecting the specific type of authenticator being used.

(2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.

SUPPLEMENTAL GUIDANCE: The CSP needs to have a documented procedure to allow subscribers to report lost or stolen physical authenticators, and to revoke or suspend such authenticators promptly when reported. Subscribers need to be instructed (see GEN-1) the procedure for reporting loss or theft.

(3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.

SUPPLEMENTAL GUIDANCE: Throttling or rate limiting is key to resistance against online guessing attacks. This is generally required for memorized secrets or when the authenticator output of a look-up secret, OOB, or OTP authenticator may have less than 64 bits of entropy.

(4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.

SUPPLEMENTAL GUIDANCE: Throttling or rate limiting is key to resistance against online guessing attacks. It is important that it be implemented in a non-abrupt manner as described in the specification so that it is not usable as a denial-of-service mechanism by an attacker. Additional techniques MAY be used to reduce the likelihood that an attacker will lock the legitimate claimant out as a result of rate limiting. These include:

- Requiring the claimant to complete a CAPTCHA before attempting authentication.
- Requiring the claimant to wait following a failed attempt for a period of time that increases as the account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour).

- Accepting only authentication requests that come from a white list of IP addresses from which the subscriber has been successfully authenticated before. Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms. These might, for example, include use of IP address, geolocation, timing of request patterns, or browser metadata.

(5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.

SUPPLEMENTAL GUIDANCE: Attestations are sometimes provided by cryptographic authenticators to securely indicate their capabilities, e.g., that they are hardware-based or that they have characteristics such as two-factor capability. For the attestations to be useful, these signatures need to use algorithms and keys that are sufficiently strong.

(6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 8 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection).

SUPPLEMENTAL GUIDANCE: In cases where the verifier and CSP are separate, it is important that this not create additional security vulnerabilities as compared with an integrated verifier/CSP combination. This requirement ensures that there is not an opportunity to perform eavesdropping or active attacks on the channel between them.

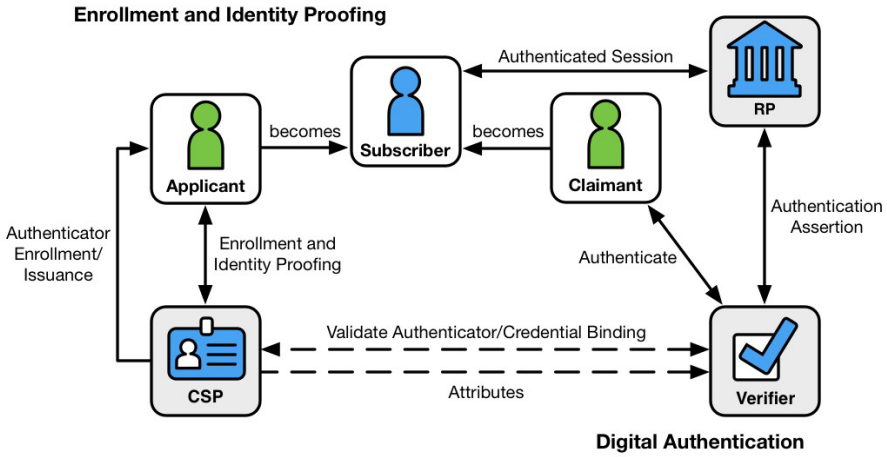


Figure 6 – Digital Identity Model

(7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.

SUPPLEMENTAL GUIDANCE: It is important that the loss of control of an authenticator be quickly reported to the CSP. To balance between the need to easily and promptly report this and the risk of a fraudulent report, a backup authenticator, either a memorized

secret or physical authenticator, should be usable by the subscriber to make this report. Only a single, single-factor authenticator is required.

(8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.

SUPPLEMENTAL GUIDANCE: Reversibility of suspension is intended to minimize the impact of inadvertent loss reports from the subscriber and in some cases from an attacker who may be attempting to deny service to the subscriber.

(9) If and when an authenticator expires, it SHALL NOT be usable for authentication.

SUPPLEMENTAL GUIDANCE: Expiration is used by some CSPs to limit the security exposure from an authenticator that is lost but the loss has not been detected/reported and revoked.

(10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.

SUPPLEMENTAL GUIDANCE: The requirement for surrender or destruction of expired authenticators minimizes the possibility that authentication with an expired authenticator will be attempted. PKI-based authenticators that are collected or known to be destroyed also do not need to be included in certificate revocation lists.

(11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.

SUPPLEMENTAL GUIDANCE: Prompt revocation ensures that unauthorized parties are not able to use the authenticator to make unauthorized access to the subscriber account. Revocation at subscriber request can affect only a single authenticator; the other classes of revocation generally affect all authenticators associated with the subscriber's account.

(12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.

SUPPLEMENTAL GUIDANCE: This requirement blocks the use of the authenticator's certified attributes in offline situations between revocation/termination and expiration

of the certification. Prompt revocation ensures that unauthorized parties are not able to use the authenticator to make unauthorized access to the subscriber account. Collection or destruction also minimizes the dependence on (and growth of) certificate revocation lists, which are not always 100% effective in accomplishing revocation, particularly in offline situations.

m. Biometric Requirements

(1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).

SUPPLEMENTAL GUIDANCE: For a variety of reasons listed here, a biometric factor is not considered to be an authenticator by itself. The risks associated with biometric factors are largely mitigated by binding the biometric with a specific physical authenticator.

- The biometric False Match Rate (FMR) does not provide confidence in the authentication of the subscriber by itself. In addition, FMR does not account for spoofing attacks.
- Biometric comparison is probabilistic, whereas the other authentication factors are deterministic.
- Biometric template protection schemes provide a method for revoking biometric credentials that is comparable to other authentication factors (e.g., PKI certificates and passwords). However, the availability of such solutions is limited, and standards for testing these methods are under development.
- Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g., facial images) with or without their knowledge, lifted from objects someone touches (e.g., latent fingerprints), or captured with high resolution images (e.g., iris patterns). While presentation attack detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the CSP and the subscriber.

(2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.

SUPPLEMENTAL GUIDANCE: This requirement ensures that biometric data that flows across the network to the verifier is protected from disclosure and that an attacker cannot substitute a “skimmer” or other fraudulent replacement for the biometric sensor. If the biometric factor is verified directly on a multi-factor authenticator and the sensor

is tightly integrated with it, that local connection does not require an authenticated protected channel.

(3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.

SUPPLEMENTAL GUIDANCE: This requirement ensures that the biometric data being verified is obtained from the expected sensor rather than from a device that may be spoofing biometric information. This is generally not required when the biometric factor is verified in an endpoint that is tightly integrated with the sensor in a manner that resists sensor replacement.

(4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1].

SUPPLEMENTAL GUIDANCE: Since biometric comparison is an approximate match, an operating point threshold is chosen by the verifier that balances false matches and false non-matches. To operate adequately as a verifier, a 1 in 1000 or better false match rate is required.

(5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.

SUPPLEMENTAL GUIDANCE: With a false accept rate of as much as 1 in 1000 zero-effort attempts, the ability to make a large number of biometric authentication attempts would result in an unacceptably high probability of mis-authentication. This limit is comparable to that provided by several commercial products (mobile devices) currently on the market.

(6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:

i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or

ii. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.

SUPPLEMENTAL GUIDANCE: Following a number of consecutive biometric match failures that exceeds the limit in IA-5 m (5), subsequent attempts need to be either aggressively delayed (e.g., 1 minute before the following failed attempt, 2 minutes before the second following attempt) or another authentication or biometric modality associated with the same physical authenticator needs to be used.

(7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.

SUPPLEMENTAL GUIDANCE: The verifier needs to have a basis for determining that biometric verification meets the necessary performance requirements. This may be accomplished by authenticating the sensor or endpoint, by a certification by an approved accreditation authority, or by runtime interrogation of a signed attestation.

(8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.

SUPPLEMENTAL GUIDANCE: The ability to use a biometric factor on an arbitrary device greatly increases the value of breached biometric data. For this reason, the use of the biometric factor is limited to specific devices for each subscriber. A separate key is required since the main authentication key is only unlocked upon successful comparison of the biometric factor.

(9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.

SUPPLEMENTAL GUIDANCE: Since the main authentication key has not yet been unlocked, a separate key is required for identifying the specific device(s) that the biometric may be used with.

(10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.

SUPPLEMENTAL GUIDANCE: Central databases of biometric templates are an attractive target for attackers. The ability to securely revoke biometric factors is required in response to that threat.

(11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.

SUPPLEMENTAL GUIDANCE: Because of the replay potential of biometric data, biometric information needs to be distributed in a manner that minimizes the opportunity for attackers to intercept the data either by eavesdropping on MitM attacks.

(12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived.

SUPPLEMENTAL GUIDANCE: If the biometric factor is used for any supplemental purpose, it is important that it not be a mechanism for breach of subscribers' biometric data.

n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account.

(1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.

SUPPLEMENTAL GUIDANCE: In the past, many physical authenticators were provided by the CSP. More recently, there has been a trend toward BYO authenticators, which can be both cost-effective for CSPs and convenient for the subscriber. This requirement ensures that such BYO authenticators are subject to approval by the CSP, primarily to ensure that they meet security requirements.

(2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.

SUPPLEMENTAL GUIDANCE: In order to authenticate subscribers successfully, the CSP needs to maintain a record of authenticators bound to each subscriber's account. In addition, a record of authenticators formerly bound to each account needs to be kept for forensic purposes.

(3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts.

SUPPLEMENTAL GUIDANCE: In order to successfully support the throttling of authentication attempts (see requirement IA-5 l (3)), the CSP needs to maintain information on the number of consecutive failed authentication attempts.

(4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.

SUPPLEMENTAL GUIDANCE: In order to determine compliance with AAL-specific requirements, the CSP needs to reliably determine some authenticator characteristics, such as whether the authenticator is hardware-based, whether it is a single-factor or multi-factor authenticator, and performance characteristics of associated biometric sensors. Mechanisms to do this include attestation certificates from the manufacturer and examination of the authenticator (particularly at account issuance). In the absence of this information, the CSP needs to assume that the authenticator is the weakest type that is consistent with the authentication protocol being used.

(5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.

SUPPLEMENTAL GUIDANCE: For forensic purposes it is useful to have a record of the period of time each authenticator is bound to the subscriber's account.

(6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.

SUPPLEMENTAL GUIDANCE: If the process of binding an authenticator is not strong enough, an authenticator that is fraudulently bound to the account could be used by an attacker to gain access to a subscriber's account. The authentication factor being bound to the account needs to be included in the authentication process for the session in which the authenticator is bound.

(7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against MitM attacks.

SUPPLEMENTAL GUIDANCE: For the same reasons that MitM attacks are of concern during authentication, they could occur during provisioning, which could result in the binding of an attacker's key to the account rather than the subscriber's key.

(8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.

SUPPLEMENTAL GUIDANCE: In order to prevent a subscriber with only single-factor authentication from up-leveling to multi-factor, binding of a multi-factor authenticator requires that the subscriber be multi-factor authenticated at the time the new authenticator is bound

(9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.

SUPPLEMENTAL GUIDANCE: Executive order 13681 requires the use of multi-factor authentication for the release of personal data. Therefore, it is important that the CSP associate sufficient authentication factors at enrollment to make this possible. While all identifying information is self-asserted at IAL1, preservation of online material or an online reputation makes it undesirable to lose control of an account due to the loss of an authenticator. The second authenticator makes it possible to securely recover from an authenticator loss. For this reason, a CSP SHOULD bind at least two physical authenticators to the subscriber's credential at IAL1 as well.

(10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.

SUPPLEMENTAL GUIDANCE: In order to support higher identity assurance, correspondingly high authenticator assurance levels are required to ensure the proper use of the identity.

(11) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.

SUPPLEMENTAL GUIDANCE: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. At this point it is not possible to fully authenticate the applicant, but the use of a temporary secret provides the necessary protection for this one-time transaction.

(12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.

SUPPLEMENTAL GUIDANCE: Long-term secrets need to be protected against disclosure while they are sent to the applicant. This applies primarily to symmetric keys, such as for OTP authenticators, that are sent to the applicant by the CSP. "Protected session" in this context refers to an authenticated protected.

(13) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter.

SUPPLEMENTAL GUIDANCE: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. At this point it is not possible to fully authenticate the applicant, but the use of a temporary secret provides the necessary protection for this one-time transaction.

(14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.

SUPPLEMENTAL GUIDANCE: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. A new secret for this purpose is required for each subsequent encounter.

(15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.

SUPPLEMENTAL GUIDANCE: To avoid misappropriation of long-term authenticator secrets at enrollment, the CSP is required to load the secrets onto authenticators directly, or deliver them to the new subscriber in a manner that confirms the address of record, typically by sending a short-term secret to that address that the new subscriber uses to obtain the long-term secret.

(16) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.

SUPPLEMENTAL GUIDANCE: In order to maintain the significance of AALs and prevent attackers from leveraging lower AAL authentication to gain access to higher AAL resources, subscribers binding additional authenticators need to do so at the maximum AAL at which they will be used.

(17) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor.

SUPPLEMENTAL GUIDANCE: This is a special-case, one-time only exception to IA-5(n)(17) to allow a single-factor account not subject to identity proofing (IAL1) to be upgraded to a multi-factor account. This provides a mechanism for such accounts to increase their authentication security.

(18) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12.

SUPPLEMENTAL GUIDANCE: Repeating the identity proofing process is an onerous requirement when a subscriber is no longer able to complete multi-factor authentication, but it is necessary to avoid the security problems typically present in "account recovery" situations. This is the primary reason that the binding of multiple authenticators is recommended, particularly in the case of physical authenticators. The entire identity

proofing process need not be repeated if the CSP has maintained enough records of the evidence presented to repeat the verification phase of identity proofing.

(19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using a n authenticator of the remaining factor, if any, to confirm binding to the existing identity.

SUPPLEMENTAL GUIDANCE: While use of an authenticator at a different factor is only a single authentication factor (and therefore only AAL1), authentication in conjunction with the repeated identity proofing process provides assurance that the claimant is who they claim to be.

(20) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.

SUPPLEMENTAL GUIDANCE: Loss of a memorized secret is different from the loss of a physical authenticator because it is not mitigated by the binding of multiple authenticators. This alternate method of associating a new memorized secret may be used by CSPs to avoid the need for repeating identity proofing (Refer to IA-12).

(21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].

SUPPLEMENTAL GUIDANCE: The confirmation code is required to have sufficient entropy and to be generated in a manner that cannot be predicted by an attacker.

(22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.

SUPPLEMENTAL GUIDANCE: The confirmation code has a limited lifetime to mitigate the risk of loss or misappropriation in transit.

o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.

Once an authentication event has taken place, it is often desirable to allow the subscriber to continue using the application across multiple subsequent interactions without requiring them

to repeat the authentication event. This requirement is particularly true for federation scenarios where the authentication event necessarily involves several components and parties coordinating across a network.

(1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).

a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.

SUPPLEMENTAL GUIDANCE: This secret binds the two ends of the session, allowing the subscriber to continue using the service over time.

b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.

SUPPLEMENTAL GUIDANCE: The session secret is considered a short-term secret, so direct presentation of a shared secret is permitted, even at AAL2 or AAL3.

c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.

SUPPLEMENTAL GUIDANCE: The session secret needs to be directly associated with authentication so that it isn't inadvertently provided to the wrong session.

d. A session SHALL NOT be considered at a higher AAL than the authentication event.

SUPPLEMENTAL GUIDANCE: Each session has an associated maximum AAL at which it can be used that is derived from the authentication AAL; this is associated with the session and its secret by the CSP/RP.

e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.

SUPPLEMENTAL GUIDANCE: It is the responsibility of the host (RP/CSP/Verifier) to generate session secrets, not the subscriber.

f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1].

SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the session secret.

g. Secrets used for session binding SHALL contain at least 64 bits of entropy.

SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the session secret.

h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.

SUPPLEMENTAL GUIDANCE: At a minimum, the CSP/RP needs to ensure that the session secret can no longer to be used following logout. If possible, the secret should be erased on the subscriber endpoint as well.

i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.

SUPPLEMENTAL GUIDANCE: Session secrets, particularly when directly presented, need to be protected against eavesdropping and MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL.

SUPPLEMENTAL GUIDANCE: This requirement is in support of the reauthentication requirements in AAL2-*, AAL3-*, and REAUTH-*. The proper way to ensure that a session is logged out is to invalidate the session secrets associated with that session. A new session secret will need to be generated and associated with any session that is about to be established from the same endpoint.

k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.

SUPPLEMENTAL GUIDANCE: User endpoints such as browsers that support both secure and insecure communications typically have mechanisms to flag information (e.g., cookies) that are only available to secure sessions. These mechanisms are required to be used for session management secrets. See also IA-5 o (7).

l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.

SUPPLEMENTAL GUIDANCE: In some cases, endpoints supporting https provide, primary for legacy purposes, the ability to connect via http as well. If not done properly, this can make the site vulnerable to a "downgrade attack" where a session switches from https to http. This must not happen for authenticated sessions. If session secrets are managed properly, this downgrade interferes with the continuity of the session.

m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.

SUPPLEMENTAL GUIDANCE: Unique session identifiers in the URL or POST content are used to ensure that sessions are not vulnerable to cross-site request forgery (CSRF). Note that the session identifier is separate and different from the session secret; under no circumstances should the session secret be included in a URL.

n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.

SUPPLEMENTAL GUIDANCE: Browser cookies have an optional "secure" flag to ensure that they are not accidentally transmitted over a non-secure channel. This flag must be set for session secrets.

o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.

SUPPLEMENTAL GUIDANCE: Browser cookies have a scope parameter that limits the sites from to which the cookie can be sent; this should be specified as specifically as possible to limit access to the session secret as narrowly as practical.

p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.

SUPPLEMENTAL GUIDANCE: While browser cookies have an expiration time, enforcement of session timeouts must occur at the RP/CSP and not at the user endpoint. Cookie expiration may, however, be used to limit accumulation of cookies in the browser.

q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.

SUPPLEMENTAL GUIDANCE: Access tokens, used in federated identity systems, may be valid after the authentication session has ended and the subscriber has left.

(2) Reauthentication Requirements

a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.

SUPPLEMENTAL GUIDANCE: This is a reiteration of requirement IA-5 o (1).

b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.

SUPPLEMENTAL GUIDANCE: Session secrets are not to be maintained across a restart of the associated application or a reboot of the host device in order to minimize the likelihood that a misappropriated logged in device can be exploited.

c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.

SUPPLEMENTAL GUIDANCE: In order to protect against a subscriber leaving a logged-in endpoint, timeouts are defined for session inactivity and overall session length. The timer for these timeouts is reset by a reauthentication transaction. Higher AALs have more stringent (shorter) reauthentication timeouts. Following expiration of the session timer, the subscriber is required to start a new session by authenticating.

d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.

SUPPLEMENTAL GUIDANCE: The existence and possession of a session secret does not consider whether the subscriber continued to be in control of the session endpoint. To mitigate this risk, the session secret is only valid for a limited period of time. While the session secret is "something you have", it is not an authenticator.

e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.

SUPPLEMENTAL GUIDANCE: Before the session times out, the subscriber should be given an opportunity to reauthenticate to extend the session. The subscriber may be prompted when an idle timeout is about to expire, to allow them to cause activity and thereby avoid the need to reauthenticate.

Note: At AAL2, a memorized secret or biometric, and not a physical authenticator, is required because the session secret is something you have, and an additional authentication factor is required to continue the session.

f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.

SUPPLEMENTAL GUIDANCE: When an RP session expires and the RP requires reauthentication, it is entirely possible that the session at the CSP has not expired and that a new assertion could be generated from this session at the CSP without reauthenticating the user.

g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP.

SUPPLEMENTAL GUIDANCE: In some applications, RPs may require a "fresh" authentication to meet its authentication risk requirements. By specifying maximum age, the RP can proactively request the CSP to obtain a new authentication to meet that requirement.

h. If federated authentication if being used and an RP has specific authentication age (see IA-5 j [10]) requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.

SUPPLEMENTAL GUIDANCE: When the RP communicates its authentication freshness requirements to the CSP, the CSP is expected to reauthenticate the subscriber to support a session that meets those requirements.

i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.

SUPPLEMENTAL GUIDANCE: When federation authentication is being used, the authentication assertion from the CSP needs to contain the authentication event time to allow the RP to request reauthentication at an appropriate interval if it has specific authentication age requirements.

DISCUSSION: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational

systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, MA-4, PE-2, PL-4, SC-12, SC-13.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES

[Priority 1]

Control:

(a) Memorized Secret Authenticators and Verifiers:

1. Maintain a list of commonly-used, expected, or compromised passwords via API or download from a third party. Update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly. Compare current memorized secrets against the list quarterly;
2. Require immediate selection of a new password upon account recovery;
3. Allow user selection of long passwords and passphrases, including spaces and all printable characters;
4. Employ automated tools to assist the user in selecting strong password authenticators;
5. If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.

   SUPPLEMENTAL GUIDANCE: Memorized secret length is the most reliable metric determining strength against online and offline guessing attacks. The objective is primarily to defend against online attacks (with throttling of guesses) and to provide some protection against offline attacks, with the primary defense for such attacks being secure storage of the verifier.

6. If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.

   SUPPLEMENTAL GUIDANCE: Memorized secret length is the most reliable metric determining strength against online and offline guessing attacks. The objective is primarily to defend against online attacks (with throttling of guesses) and to provide some protection against offline attacks, with the primary defense for such attacks being secure storage of the verifier.

7. Truncation of the secret SHALL NOT be performed.

SUPPLEMENTAL GUIDANCE: Memorized secrets that are longer than expected by the verifier might (but must not) be simply truncated to an acceptable length. This gives a false impression of security to the user if the verifier only checks a subset of the memorized secret.

8. Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.

   SUPPLEMENTAL GUIDANCE: The availability of memorized secret hints greatly weakens the strength of memorized secret authenticators.

9. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.

   SUPPLEMENTAL GUIDANCE: Prompts for specific information (often called Knowledge-based Authentication or Security Questions) encourage use of the same memorized secrets at multiple sites, which causes a vulnerability to "password stuffing" attacks. This guidance applies to account recovery situations as well as normal authentication.

10. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against the list maintained as required by IA-5(1)(a)(1) that contains values known to be commonly used, expected, or compromised.

    SUPPLEMENTAL GUIDANCE: The maintenance of a list of common memorized secrets that cannot be used by users protects provides protection against online attacks that might otherwise succeed before throttling mechanisms take effect to defend against these attacks. This is an alternative to the use of composition rules (requirements for particular character types, etc.) and can provide more customized protection against common memorized secrets. This list may include, but is not limited to:

    - Passwords obtained from previous breach corpuses.
    - Dictionary words.
    - Repetitive or sequential characters (e.g., 'aaaaaa', '1234abcd').
    - Context-specific words, such as the name of the service, the username, and derivatives thereof.

11. If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.

    SUPPLEMENTAL GUIDANCE: The use of common memorized secrets greatly increases the vulnerability of the account to both online (guessing) and offline (cracking) attacks. This is an alternative to the use of composition rules (requirements for particular character

types, etc.) and can provide more customized protection against common memorized secrets.

12. If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.

    SUPPLEMENTAL GUIDANCE: When a subscriber chooses a weak memorized secret, it is likely that they will choose another weak memorized secret that may or may not be on the blocklist. In addition to explaining to the user the reason for the rejection of their selection, it is helpful to provide coaching on better choices. Tools like password-strength meters are often useful in this situation.

13. If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.

    SUPPLEMENTAL GUIDANCE: When a subscriber chooses a weak memorized secret, the memorized secret change process is not complete until the subscriber has chosen a different value.

14. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.

    SUPPLEMENTAL GUIDANCE: Rate limiting restricts the ability of an attacker to make many online guessing attacks on the memorized secret. Other requirements (e.g., minimum length of memorized secrets) depend on the existence of rate limiting, so effective rate limiting is an essential capability. Ideally, a rate limiting mechanism should restrict the attacker as much as possible without creating an opportunity for a denial-of-service attack against the subscriber.

15. Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.

    SUPPLEMENTAL GUIDANCE: Although requiring routine periodic changes to memorized secrets is not recommended, it is important that verifiers have the capability to prompt memorized secrets on an emergency basis if there is evidence of a possible successful attack.

16. The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.

    SUPPLEMENTAL GUIDANCE: As defined in Appendix A of the CJIS Security Policy, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

17. The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.

    SUPPLEMENTAL GUIDANCE: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

18. Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.

    SUPPLEMENTAL GUIDANCE: Storage of memorized secret verifiers in a hashed form that is not readily reversed is a key protection against offline attacks. In no case should a verifier store memorized secrets in cleartext form. Criteria IA-5(1)(a)(20) – (22) provide more detail on how this is done.

19. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.

    SUPPLEMENTAL GUIDANCE: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive. Use of a key derivation with a salt, preferably with a time- and memory-hard key derivation function, provides the best protection against attackers that are able to obtain a copy of the verifier database.

20. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

    SUPPLEMENTAL GUIDANCE: Salt values need to be large enough to make it impractical for an attacker to precompute hashed verifier values (so called rainbow tables). While rainbow tables are typically quite large, this requirement would increase their size by a factor of about 4.3 billion. If not chosen arbitrarily, the attacker might be able to anticipate the salt values that would be used, which would eliminate much of this advantage.

21. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator

    SUPPLEMENTAL GUIDANCE: In order to verify a memorized secret, it needs to be salted and hashed for comparison with the stored verifier (resulting hash). To do this, the salt value needs to be available, and since it is different for each user, needs to be stored with the verifier. It is impractical to verify a memorized secret if this is not done.

22. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.

    SUPPLEMENTAL GUIDANCE: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers ("password crackers") with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be generated in a manner that is not vulnerable to compromise.

23. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.

    SUPPLEMENTAL GUIDANCE: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers ("password crackers") with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be of sufficient size to make cryptographic and brute-force attacks impractical.

    Currently, the requirement is that the key be at least 112 bits in length.

24. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.

    SUPPLEMENTAL GUIDANCE: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers ("password crackers") with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be stored separately so that it is unlikely to be compromised along with the verifier database. One way to do this is to perform this last hashing iteration on a physically separate processor, since it only requires a value to hash as input and provides the hashed value in response.

DISCUSSION: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(a)(5). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses,

dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

(b) Look-Up Secret Authenticators and Verifiers

1. CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.

   SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the look-up secret

2. Look-up secrets SHALL have at least 20 bits of entropy.

   SUPPLEMENTAL GUIDANCE: Look-up secrets need to have enough entropy to ensure that brute-force guessing attacks do not succeed.

3. If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 ‘n’ 17 through 25.

   SUPPLEMENTAL GUIDANCE: Look-up secrets need to be distributed in a manner that minimizes the opportunity for attackers to intercept the secrets either by eavesdropping or MitM attacks.

4. Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.

   SUPPLEMENTAL GUIDANCE: In most cases claimants will be prompted for the next unused memorized secret in a list but may be challenged to use a specific secret from a list.

5. A given secret from an authenticator SHALL be used successfully only once.

   SUPPLEMENTAL GUIDANCE: Many threats, such as key logging, are enabled if the look-up secret can be used more than once.

6. If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.

   SUPPLEMENTAL GUIDANCE: Grid (bingo) cards are sometimes used to provide a rudimentary challenge-response authentication involving the claimant. However, an attacker such as a key logger that has persistent access to the endpoint can derive the contents of the grid, and potentially authenticate successfully, if grid entries are reused in subsequent authentication transactions.

   Absent the ability to reuse grid squares, grid (bingo) cards will probably no longer be attractive as authenticators.

7. Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.

   SUPPLEMENTAL GUIDANCE: Storage of look-up secret verifiers in a hashed form that is not readily reversed is a key protection against offline attacks. In no case should a verifier store look-up secrets in cleartext form.

8. If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function

   SUPPLEMENTAL GUIDANCE: Use of an approved one-way function effectively protects the look-up secrets from disclosure if the verifier is compromised. Salting of secrets with this amount of entropy is not required because it is not practical to mount brute-force or cryptographic attacks against secrets this large.

9. If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.

   SUPPLEMENTAL GUIDANCE: Key derivation functions take a look-up secret, a salt, and a cost factor as inputs then generate a hash. Their purpose is to make each look-up secret guessing trial by an attacker who has obtained a look-up secret hash file expensive and therefore the cost of a guessing attack high or prohibitive. Use of a key derivation with a salt, preferably with a time- and memory-hard key derivation function, provides the best protection against attackers that are able to obtain a copy of the verifier database.

10. If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

    SUPPLEMENTAL GUIDANCE: Salt values need to be large enough to make it impractical for an attacker to precompute hashed verifier values (so called rainbow tables). While rainbow tables are typically quite large, this requirement would increase their size by a factor of about 4.3 billion. If not chosen arbitrarily, the attacker might be able to anticipate the salt values that would be used, which would eliminate much of this advantage.

11. If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret.

    SUPPLEMENTAL GUIDANCE: In order to verify a look-up secret, it needs to be salted and hashed for comparison with the stored verifier (resulting hash). To do this, the salt value needs to be available, and since it is different for each secret, needs to be stored with the verifier. It is impractical to verify a look-up secret if this is not done.

12. If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.

    SUPPLEMENTAL GUIDANCE: Rate limiting restricts the ability of an attacker to make many online guessing attacks on the look-up secret. Other requirements (e.g., minimum length of look-up secrets) depend on the existence of rate limiting, so effective rate limiting is an essential capability. Ideally, a rate limiting mechanism should restrict the attacker as much as possible without creating an opportunity for a denial-of-service attack against the subscriber.

13. The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

    SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

14. The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

    SUPPLEMENTAL GUIDANCE: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

(c) Out-of-Band Authenticators and Verifiers

1. The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.

   SUPPLEMENTAL GUIDANCE: A channel is considered to be out-of-band with respect to the primary communication channel (even if it terminates on the same device) provided the device does not leak information from one channel to the other without the authorization of the claimant.

2. Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).

   SUPPLEMENTAL GUIDANCE: The secondary channel requires protection to ensure that authentication secrets are not leaked to attackers. Legacy use of the PSTN as an OOB authentication medium is exempt from this requirement, although other requirements apply.

3. Methods that do not prove possession of a specific device, such as voice-over-IP (VoIP) or email, SHALL NOT be used for out-of-band authentication.

SUPPLEMENTAL GUIDANCE: Communication with VoIP phone numbers and email do not establish the possession of a specific device, so they are not suitable for use in out-of-band authentication which is used as a physical authenticator (something you have).

4. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.

   SUPPLEMENTAL GUIDANCE: Communication between out-of-band device and verifier is required to be via an encrypted channel to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

5. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.

   SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

6. If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).

   SUPPLEMENTAL GUIDANCE: The secret key associated with an out-of-band device or authenticator application is critical to the determination of "something you have" and needs to be well protected.

7. If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.

   SUPPLEMENTAL GUIDANCE: Since the PSTN does not support the establishment of authenticated protected channels, the alternative method of authenticating the device via the PSTN is supported. Note that there are other specific requirements for use of the PSTN that also apply (see IA-5 (1) c (19) through (20)).

8. If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.

SUPPLEMENTAL GUIDANCE: Most out-of-band verifiers operate by sending a secret over the secondary channel that the subscriber transfers to the primary channel (e.g., the capability to copy and paste from one app to another). Other methods are possible, however, specifically transferring from primary to secondary and user comparison of secrets sent to both channels (with approval being sent to the verifier over the secondary channel). It is good practice to display descriptive information relating to the authentication on the claimant's out-of-band device, to provide additional assurance that the transaction being approved by the subscriber is the correct one, and not from an attacker who exploits the subscriber's approval.

9. The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.

   SUPPLEMENTAL GUIDANCE: In order for the out-of-band authenticator to be considered "something you have", it must be securely authenticated as a unique device or instance of a software-based authentication application. This is required to be done through proof of possession of a key by the authenticator, rather than presentation of the key itself. This provides verifier compromise resistance with respect to the authentication key.

10. Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.

    SUPPLEMENTAL GUIDANCE: Three different methods of associating the primary and secondary channel sessions are permitted. The intent of these methods is to establish approval for a specific authentication transaction, and to minimize the likelihood that an attacker with knowledge of when the subscriber authenticates can obtain approval for a rogue authentication.

11. If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.

    SUPPLEMENTAL GUIDANCE: This is the most common form of out-of-band authentication where an authentication secret is transmitted to the out-of-band device and entered by the user for transmission on the primary channel.

12. If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.

SUPPLEMENTAL GUIDANCE: This is a less typical authentication flow but is also acceptable in that the secret securely associates possession and control of the out-of-band authenticator with the session being authenticated.

13. If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.

    SUPPLEMENTAL GUIDANCE: This is a somewhat more user-friendly authentication flow because it does not require the claimant to read and manually enter the authentication secret, but it carries the additional risk that the claimant will approve the authentication without actually comparing the secrets received from the independent channels. Approval is required to be obtained from the out-of-band authenticator rather than the primary channel because that at least establishes control of the authenticator.

14. The authentication SHALL be considered invalid if not completed within 10 minutes.

    SUPPLEMENTAL GUIDANCE: Secrets used in out-of-band authentication are short-term secrets and need to have a definite lifetime. This requirement also relieves the verifier from the responsibility of log-term storage of the secrets.

15. Verifiers SHALL accept a given authentication secret only once during the validity period.

    SUPPLEMENTAL GUIDANCE: In order to prevent an attacker who gains access to an authentication secret generated by the subscriber from using it, it is important that the secret only be valid for a single authentication. This requirement only applies when a secret is being transferred between the primary channel and the out-of-band authenticator.

16. The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.

    SUPPLEMENTAL GUIDANCE: Consistent with other short-term authentication secrets, 20 bits of entropy are required to provide resistance against brute force attacks. 6-digit numeric secrets (19.93 bits of entropy) are sufficiently close to 20 bits to be acceptable.

17. The verifier SHALL generate random authentication secrets using an approved random bit generator.

    SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the out-of-band secret. Approved random bit generators are generally included in a FIPS 140-2 certified encryption module.

18. If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

    SUPPLEMENTAL GUIDANCE: Rate limiting limits the opportunity for attackers to mount a brute-force attack on the out-of-band verifier. Since the out-of-band secret has a limited lifetime, it is sufficient to limit the number of attempts allowed during the (maximum) 10-minute lifetime of the secret.

19. If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.

    SUPPLEMENTAL GUIDANCE: Some telephone numbers, such as those that are associated with VoIP services, are not associated with a specific device and can receive calls and text messages without establishing possession and control of a specific device. Such telephone numbers are not suitable for OOB authentication. Services exist to distinguish telephone numbers that are associated with a device from those that aren't.

20. If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).

    SUPPLEMENTAL GUIDANCE: The binding of a new authenticator requires that the subscriber authenticate at the same or a higher AAL (currently AAL2) than that at which the authenticator will be used, and that a notification be sent to the subscriber. This is required to prevent attackers from changing the phone number of a PSTN-based out-of-band authenticator to one they control.

21. If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.

    SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. CSPs are required to provide subscribers with a meaningful alternative.

22. If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.

SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. CSPs are required to explain these risks to subscribers and offer more secure alternatives.

Currently, authenticators leveraging the public switched telephone network, including phone- and Short Message Service (SMS)-based one-time passwords (OTPs) are restricted. Other authenticator types may be added as additional threats emerge. Note that, among other requirements, even when using phone- and SMS-based OTPs, the agency also must verify that the OTP is being directed to a phone and not an IP address, such as with VoIP, as these accounts are not typically protected with multi-factor authentication.

23. If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.

    SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. These risks need to be documented.

24. If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.

    SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. A plan for eliminating them in the future needs to be documented.

(d) OTP Authenticators and Verifiers

1. The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.

   SUPPLEMENTAL GUIDANCE: The secret key used by an OTP authenticator needs to be sufficiently complex to resist online and offline attacks. An attacker may have the ability to observe the authenticator output at some point during its operation; it needs to be impractical for the secret key to be derived from a set of these observations.

2. The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

   SUPPLEMENTAL GUIDANCE: If the nonce isn't long enough, the output of the authenticator will repeat, which represents an easily avoided vulnerability.

3. OTP authenticators — particularly software-based OTP generators —SHALL NOT facilitate the cloning of the secret key onto multiple devices.

SUPPLEMENTAL GUIDANCE: Like other physical authenticators, the use of OTP authenticators is premised upon the authenticator secret being present in a single authenticator so that it proves possession of a specific device. Mechanisms that would facilitate cloning the secret onto multiple devices include the ability to enroll more than one device producing the same OTP output and backup mechanisms, especially when software-based authenticators are used. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

4. The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.

   SUPPLEMENTAL GUIDANCE: Consistent with other short-term authentication secrets, 20 bits of entropy are required to provide resistance against brute force attacks. 6-digit numeric secrets (19.93 bits of entropy) are sufficiently close to 20 bits to be acceptable.

5. If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.

   SUPPLEMENTAL GUIDANCE: The authenticator output needs to be changed often enough that there is reasonable assurance that it is in the possession of the claimant and that it is not susceptible to OTP-guessing attacks.

6. The OTP value associated with a given nonce SHALL be accepted only once.

   SUPPLEMENTAL GUIDANCE: A fundamental premise of a "one-time" authenticator is that it can be used successfully only once during its validity period.

7. The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.

   SUPPLEMENTAL GUIDANCE: Verifiers typically contain symmetric keys for all subscribers using OTP authenticators. This makes them a particularly rich target for attackers. While the protection of these keys is implementation- dependent and there is therefore no specific requirement for how the keys are protected, measures to prevent the exfiltration of the keys are needed. An example of such a measure is the storage of keys and generation of authenticator outputs in a separate device accessible only by the verifier.

8. If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.

   SUPPLEMENTAL GUIDANCE: It is critical that authentication secrets be generated and transferred or negotiated securely. This includes the use of secure random number generators and protocols for transferring or negotiating (e.g., Diffie-Hellman) secret values.

Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

9. The verifier SHALL use approved encryption when collecting the OTP.

   SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

10. The verifier SHALL use an authenticated protected channel when collecting the OTP.

    SUPPLEMENTAL GUIDANCE: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

11. If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.

    SUPPLEMENTAL GUIDANCE: The clocks on time-based authenticators are subject to drift because of cost and environmental factors such as temperature. Accordingly, verifiers need to accept authenticator outputs before and particularly after the intended validity period to allow use by authenticators that are not in synchronization.

12. Verifiers SHALL accept a given time-based OTP only once during the validity period.

    SUPPLEMENTAL GUIDANCE: In order to prevent an attacker who gains access to an OTP authenticator output from using it, it is important that the secret only be valid for a single authentication.

13. If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

    SUPPLEMENTAL GUIDANCE: OTPs whose output has less entropy are more vulnerable to online guessing attacks. To mitigate these attacks, rate limiting is required. Online guessing attacks are less of a concern for time-based OTP authenticators because of the limited validity window, but a limit on the number of guesses during a given validity period is effective in resisting automated attacks.

14. If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.

SUPPLEMENTAL GUIDANCE: To ensure that a multi-factor authenticator cannot be stolen and used repeatedly following activation, a separate activation is required for each use of the authenticator. It is preferable for a multi-factor authenticator not to indicate that the wrong memorized secret or biometric were presented, but rather to produce an authenticator output that is invalid, although this is not required. This provides protection against guessing or presentation attacks on the authenticator itself.

15. If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a).

    SUPPLEMENTAL GUIDANCE: The requirement for memorized secrets used as activation factors is the same as that for memorized secrets used as distinct authenticators (see IA-5 (1)(a)).

16. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).

    SUPPLEMENTAL GUIDANCE: Rate limiting is required to provide protection against brute-force guessing attacks, particularly if the authenticator gives an indication when an incorrect secret is entered.

17. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

    SUPPLEMENTAL GUIDANCE: General requirements for biometric activation factors include false accept rate criteria and the number of consecutive authentication failures that are allowed.

18. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.

    SUPPLEMENTAL GUIDANCE: It is important that the unencrypted key and associated data be zeroized to minimize the likelihood that it can be misappropriated by an attacker following a successful authentication. Each authentication requires a re-presentation of the activation factor (see IA-5(1)(d)14). Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

19. If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.

    SUPPLEMENTAL GUIDANCE: From the standpoint of a verifier, a multi-factor OTP authenticator appears the same as a single-factor OTP authenticator. In order to establish that the authenticator meets the multi-factor requirements, the verifier or CSP can issue the authenticator, examine it in some way, or rely on an assertion from the manufacturer.

20. In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).

    SUPPLEMENTAL GUIDANCE: Authenticators of unknown provenance or that are not known by the CSP or verifier to meet all of the requirements for multi-factor OTP authenticators can be used, but only as single-factor authenticators.

(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)

1. If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.

   SUPPLEMENTAL GUIDANCE: Although dependent on the computing device on which the authenticator is operating, authenticator software needs to avail itself of the most secure storage available, considering issues like ability to extract the secret from the device and its potential to be included in backup data. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

2. If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.

   SUPPLEMENTAL GUIDANCE: Although dependent on the computing device on which the authenticator is operating, authenticator software needs to store secret keys in a manner that limits access to keys to the maximum extent possible so that they cannot be accessed by other (possibly rogue) applications and/or users. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

3. If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.

   SUPPLEMENTAL GUIDANCE: Like other physical authenticators, the use of cryptographic authenticators is premised upon the authenticator secret being present in a single authenticator so that it proves possession of a specific device. Mechanisms that would facilitate cloning the secret onto multiple devices include the ability to enroll more

than one device with the same key and backup mechanisms, especially when software-based authenticators are used. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

4. If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).

   SUPPLEMENTAL GUIDANCE: Cryptographic device authenticators are constructed so as not to allow the secret key to be obtained from the device. These devices are enrolled for authentication using the public cryptographic key, but the private key is never shared. This requirement addresses primarily functionality allowing the key to be exported; FIPS 140 requirements cover the resistance of the device to various forms of attack.

5. If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.

   SUPPLEMENTAL GUIDANCE: The secret key used by a cryptographic authenticator needs to be sufficiently complex to resist online and offline attacks. An attacker may have the ability to observe the authenticator output at some point during its operation; it needs to be impractical for the secret key to be derived from a set of these observations. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

6. If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.

   SUPPLEMENTAL GUIDANCE: This requirement applies to hardware-based cryptographic authenticators. The challenge nonce is required to be large enough that it will not be reused during the lifetime of the authenticator in order to provide replay protection. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the nonce generated by the verifier also assesses the authenticators that may be used.

7. If the authenticator is hardware-based, approved cryptography SHALL be used.

   SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

8. Cryptographic keys stored by the verifier SHALL be protected against modification.

   SUPPLEMENTAL GUIDANCE: Protection against modification is required for all keys to ensure that an attacker can't substitute keys they control, which would permit them to

authenticate successfully. This protection could be provided by operating system access controls, or through integrity checks of the stored keys with separately stored hashes.

9. If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.

   SUPPLEMENTAL GUIDANCE: Protection against disclosure is required for symmetric keys because their disclosure also would permit an attacker to authenticate successfully. This protection could be provided through operating system access controls.

10. The challenge nonce SHALL be at least 64 bits in length.

    SUPPLEMENTAL GUIDANCE: This requirement applies to verifiers of cryptographic authentication. The challenge nonce is generated by the verifier and used by a cryptographic authenticator to compute the authenticator output. The challenge needs to be sufficiently long that it will not need to repeat during the lifetime of the authenticator, so the authenticator output, if available to an attacker, cannot be replayed.

11. The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).

    SUPPLEMENTAL GUIDANCE: The challenge nonce is generated by the verifier used by a cryptographic authenticator to compute the authenticator output. The nonce cannot repeat during the lifetime of the authenticator, so the authenticator output, if available to an attacker, cannot be replayed. This can be accomplished by either deterministic means (e.g., an algorithm choosing values guaranteed not to repeat) or statistically (random values chosen from a range giving a very low probability that the same nonce will ever be seen twice).

12. The verification operation SHALL use approved cryptography.

    SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

13. If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.

    SUPPLEMENTAL GUIDANCE: The activation factor, either a memorized secret or a biometric, is required to be presented each time an authentication operation is requested by the authenticator to ensure that an activated authenticator cannot be used by an attacker.

14. If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).

    SUPPLEMENTAL GUIDANCE: The requirement for memorized secrets used as activation factors is the same as that for memorized secrets used as distinct authenticators (see IA-5(1)a).

15. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).

    SUPPLEMENTAL GUIDANCE: Rate limiting is required to provide protection against brute-force guessing attacks, particularly if the authenticator gives an indication when an incorrect secret is entered.

16. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

    SUPPLEMENTAL GUIDANCE: General requirements for biometric activation factors include false accept rate criteria and the number of consecutive authentication failures that are allowed.

17. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.

    SUPPLEMENTAL GUIDANCE: It is important that the unencrypted key and associated data be zeroized to minimize the likelihood that it can be misappropriated by an attacker following a successful authentication. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

Related Controls: IA-6.

Control Enhancements:

(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY BASED AUTHENTICATION

[Existing] [Priority 1]

Control:

(a) For public key-based authentication:

1. Enforce authorized access to the corresponding private key; and

2. Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
2. Implement a local cache of revocation data to support path discovery and validation.

DISCUSSION: Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network. A local cache of revocation data is also known as a certificate revocation list. This list contains a list of revoked certificates and can be periodically downloaded to ensure certificates can still be checked for revocation when network access is not available or access to the Online Certificate Status Protocol (OCSP) server is not available. Without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates).

Related Controls: IA-3, SC-17.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

[Existing] [Priority 1]

Control:

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

DISCUSSION: For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Related Controls: RA-2.

IA-6 AUTHENTICATION FEEDBACK

[Existing] [Priority 3] Control:

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

DISCUSSION: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as

shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

Related Controls: AC-3.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

[Priority 2]

Control:

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

DISCUSSION: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

[Priority 2]

Control:

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

DISCUSSION: Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and practicality—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-11, MA-4, RA-3, SA-4, SC-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

[Priority 2]

Control:

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.

DISCUSSION: Acceptance of Personal Identity Verification (PIV) credentials from other federal or SLTT agencies applies to both logical and physical access control systems. PIV credentials are those credentials issued by federal or SLTT agencies that conform to FIPS Publication 201 and supporting guidelines.

Related Controls: PE-3.

(2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS

[Priority 2]

Control:

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

DISCUSSION: Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with the CJISSECPOL. Approved external authenticators meet or exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding Federal requirements allows Federal Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.

Related Controls: None.

(4) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES

[Priority 2]

Control:

Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.

DISCUSSION: Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the Federal Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: None.

IA-11 RE-AUTHENTICATION

[Priority 2]

Control:

Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours.

DISCUSSION: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators, or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Related Controls: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

IA-12 IDENTITY PROOFING

[Priority 2]

Control:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

DISCUSSION: Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Organizations may be subject to laws, executive orders, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Control Enhancements:

(2) IDENTITY PROOFING | IDENTITY EVIDENCE

[Priority 2]

Control:

Require evidence of individual identification be presented to the registration authority.

DISCUSSION: Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable

evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

Related Controls: None.

(3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION

[Priority 2]

Control:

a. Require that the presented identity evidence be validated and verified through agency-defined resolution, validation, and verification methods.

DISCUSSION: Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the users account.

b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.

SUPPLEMENTAL GUIDANCE: The sole objective of identity proofing is to ensure the applicant is who they claim to be to a stated level of certitude.

c. 1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.

2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.

SUPPLEMENTAL GUIDANCE: The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes necessary to resolve to a unique individual. It provides the CSP an important starting point in the overall identity proofing process, to include the initial detection of potential fraud, but in no w a y represents a complete and successful identity proofing transaction.

Collection of PII may include attributes are used to correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions. There may be many different sets that suffice as the minimum, so it is recommended that CSPs choose this set to balance privacy and the user's usability needs, as well as the likely attributes needed in future uses of the digital identity.

Examples of attributes that may be used for minimum identity attribute sets include:

- Name (first, last. middle) with combinations and variations,
- Address (#, Street, City, County, State, Zip code) with combinations and variations,

- Date of birth (DDMMYYYY) with combinations and variations,
- Email address,
- Phone number.

For population sets that are more defined than the general population (e.g., military veterans, Native Americans), these minimum attribute sets may be tailored to that specific community.

Additionally, it is recommended that CSPs document which alternative attributes it will accept in cases where an applicant cannot provide the minimum necessary attributes (e.g., applicant does not have a home address or phone number).

d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.

SUPPLEMENTAL GUIDANCE: Notice of proofing may contain at a minimum:

- Attribute information that is mandatory
- Attribute information that is voluntary
- What will be done with the information collected
- How the information will be protected
- Consequence of not providing mandatory attribute information (e.g., suspension/termination of the identity proofing process).

This notice may be delivered as an online screen (for remote identity proofing), a poster or printed notice at in-person proofing locations, or an oral notice delivered at the time of information collection.

e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.

SUPPLEMENTAL GUIDANCE: Predictability and manageability measures include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes.

Predictability is meant to build trust and provide accountability and requires full understanding (and disclosure) of how the attribute information will be used. Manageability also builds trust by demonstrating a CSPs ability to control attribute information throughout processing – collection, maintenance, retention.

f. If the CSP employs consent as part of its measures to maintain predictability and manageability, …then it SHALL NOT make consent for the additional processing a condition of the identity service.

SUPPLEMENTAL GUIDANCE: Consent involves collecting and recording an affirmative response from the applicant that they agree to the additional processing of their attributes. In order to make this consent meaningful, it is recommended that CSPs first disclose to its applicants which attributes are being collected and processed and why.

g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.

These [redress] mechanisms SHALL be easy for applicants to find and use.

SUPPLEMENTAL GUIDANCE: The Privacy Act requires federal CSPs that maintain a system of records to follow procedures to enable applicants to access and, if incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable SORN(s), which provide the applicant with instructions on how to make a request for access or correction. It is recommended that non-federal CSPs have comparable procedures, including contact information for any third parties if they are the source of the information.

It is recommended that CSPs make the availability of any alternative methods for completing the identity proofing and enrollment processes clear to users (e.g., in person at a customer service center, if available) in the event an applicant is unable to properly complete the initial identity proofing and enrollment process requirements online.

Note: If the ID proofing process is not successful, it is recommended that CSPs inform the applicant of the procedures to address the issue but avoid informing the applicant of the specifics of why the registration failed.

To be effective, the use of a CSP's redress mechanism results in a timely correction of errors, resolution of the dispute or complaint, and the process should not be overly burdensome or complex.

It is recommended that the CSP document and publish, in a manner which is easy for Applicants to find and use, its mechanisms for redress of Applicant complaints or problems arising from the identity proofing processes.

h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.

SUPPLEMENTAL GUIDANCE: "Effective" in this requirement means that use of the redress mechanism will result in a timely correction of errors, resolution of the dispute or complaint, and the process shall not be overly burdensome or complex.

It is recommended that CSPs maintain a record or log of all cases – including outcomes – where applicants have sought redress for complaints or problems arising from the identity proofing and provide for the periodic review of these records.

i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities.

SUPPLEMENTAL GUIDANCE: Having documented procedures is a prerequisite for transparency, accountability, quality control, auditability, and ease of interoperability among federated communities. The documentation, dissemination, review and update to identity and authentication processes is a core control under IA-1 Identification and Authentication Policy and Procedures.

j. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.

SUPPLEMENTAL GUIDANCE: "Proofing errors" in this context refer to circumstances that result in the inability or failure to complete the identity proofing and enrollment processes. Such circumstances may include:

- Applicant abandons the identity proofing and enrollment processes;
- Applicant fails to provide mandatory attribute information;
- Identity evidence of required strength is not provided;
- Identity evidence is rejected following inspection;
- Identity evidence and information do not correlate;
- Information from identity evidence is not validated by issuing or authoritative sources at the required strength;
- Identity evidence verification of binding to the applicant fails; and
- Applicant fails to confirm enrollment code within code validity period.

Depending on the circumstances above, it is recommended that the documentation include the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud countermeasures when anomalies are detected. Additional controls for handling identity proofing errors include:

- Advising the applicant of identity proofing failure and recourse options; and,
- Recording the errors in enrollment records/audit logs, along with any mitigating actions.

k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.

SUPPLEMENTAL GUIDANCE: Ideally, the CSP's identity system includes the capability to securely record and log key security-related activities associated with the identity proofing process.

Examples of key steps that may be recorded in enrollment logs include:

- Identity information collected;
- Identity evidence provided;
- Identity evidence validated;
- Identity evidence validation source;
- Identity evidence binding verification method;
- Identity evidence verification result;
- Enrollment code confirmation result;
- enrollment result; and
- Authenticator enrollment binding

l. The CSP SHALL record the types of identity evidence presented in the proofing process.

SUPPLEMENTAL GUIDANCE: Ideally, the CSP's identity system includes the capability to securely record and log specific activities associated with the identity proofing process. For each piece of evidence collected or captured, the record should include:

1. Evidence type;
2. Determined strength;
3. Issuing source; and
4. Method of collection/capture*.

* Methods of collection and capture may include camera, flatbed scanner, bar code scanner.

m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:

1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;
2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and
3. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).

SUPPLEMENTAL GUIDANCE: In accordance with its risk management processes, CSPs should conduct – and document the results of – privacy and security risk assessments. It is recommended that the scope of this assessment includes risks associated with:

- Any steps the CSP takes to verify applicant identities beyond what is required by the CJISSECPOL
- The CSP's collection, processing, and protection of PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing;
- Retention and/or disposal of any records; and
- Adherence to any applicable federal requirements, laws, regulations or policies.

n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.

SUPPLEMENTAL GUIDANCE: Unauthorized disclosure of PII can result in tangible and intangible harms to both the CSP as well as the subjects of the PII. After assessing the risks associated with collecting PII as part of its enrollment process, it is recommended that the CSP employ functional and technical mechanisms that adequately protect the confidentiality, integrity, and attribution of the PII under its control.

Such mechanisms may include:

- Limiting access to PII data;
- Privacy protecting policies;
- The use of encryption for data at rest and during transmission; and
- Integrity protection mechanisms such as hashes and record access logging.

o. "The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. "

SUPPLEMENTAL GUIDANCE: An encrypted communication channel uses approved cryptography where the connection initiator (client) has authenticated the recipient (server). Authenticated protected channels provide confidentiality and MitM attack protection and are frequently used in the user authentication process. Transport Layer Security* (TLS) is an example of an authenticated protected channel where the certificate presented by the recipient is verified by the initiator. Unless otherwise specified, authenticated protected channels do not require the server to authenticate the client.

Authentication of the server is often accomplished through a certificate chain leading to a trusted root rather than individually with each server.

*TLS version 1.2 or greater is recommended.

p. "If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. "

Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above.

SUPPLEMENTAL GUIDANCE: This is a conditional requirement. CSPs may choose to obtain additional confidence in the identity proofing process beyond the requirements for IAL2 through additional fraud mitigation measures. Such measures may include:

- inspecting metadata information, such as by checking geolocation data associated with a mobile device used to send a photo or receive an SMS;
- examining the applicant's device characteristics;
- evaluating behavioral characteristics, such as typing mannerisms, gait, or voice characteristics; and
- checking against authoritative sources, such as the Death Master File.

Employing one or more of these fraud mitigation techniques may result in the collection of additional PII about an applicant. Additional PII increases the potential impact of the unauthorized disclosure of this data. As part of the privacy risk assessment on these additional fraud mitigation measures, it is recommended that CSPs consider, at a minimum, the additional data (PII) that is processed, the implications of retaining this additional PII, and ways the associated risks can be minimized without negating the effects of the additional measures.

These additional fraud mitigation measures are not intended to substitute or replace the mandatory requirements. CSPs employing these measures are still responsible for meeting all applicable requirements.

q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.

SUPPLEMENTAL GUIDANCE: This is a conditional requirement for CSPs that cease to perform identity proofing and enrollment functions. The CSP is responsible for the proper handling, protection, and retention or disposal of any sensitive data it collects, even after it ceases to provide identity proofing and enrollment services. A CSP may document its policies and procedures to the management of the data it collects in a data handling plan or other document. Additionally, it is recommended that CSPs document any specific retention policies they are subject to, in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.

Specifically, it is recommended that the CSP defines and documents the practices it has in place for fully disposing of or destroying any sensitive data including PII, or its continued protection from unauthorized access for the duration of any period of retention.

r. Regardless of whether the CSP is a federal agency or non-federal entity, the following requirements apply to the federal agency offering or using the proofing service:

1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to

conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.
2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.
3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.
4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.

SUPPLEMENTAL GUIDANCE: This requirement applies to Federal agencies whether providing authentication services directly or through a commercial provider. This requirement directs Agencies to consult with their Senior Agency Official for Privacy (SAOP) and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the Privacy Act of 1974 or the requirements of the E-Government Act of 2002. Based on this consultation and analysis, the agency may need to publish a System of Records Notice (SORN) and/or a Privacy Impact Assessment (PIA) to cover such collections, as applicable. While this requirement specifically applies only to federal agencies, CSPs that provide services to federal agencies may be expected to provide information about their identity services in support of an Agency's privacy analysis and PIA.

s. An enrollment code SHALL be comprised of one of the following:
   1 Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR
   2 A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.

SUPPLEMENTAL GUIDANCE: The use of an enrollment code for address confirmation is a requirement for IAL2 remote identity proofing and enrollment. CSPs that perform in-person identity at IAL2 may voluntarily choose to use enrollment codes for such binding, but this is not required. Enrollment codes may also be used for in-person proofing and enrollment processes if an authenticator(s) is not registered to the subscribers' account at the time of in-person identity proofing and, therefore, the authenticator binding would need to occur at a later time. Enrollment codes may be used for authenticator binding to subscribers' accounts in such circumstances.

Enrollment code use for IAL2 remote identity proofing allows the CSP to confirm that the applicant controls a validated address of record. Authenticator binding may not be completed in the same session for in-person identity proofing. Enrollment codes may be used for binding an authenticator to subscribers' accounts at a later time in such circumstances. The requirements presented in this criterion apply to all enrollment codes that may be used by the CSP for any purpose.

Enrollment code use has the additional requirement for code validity periods. The validity period is determined by the type of address where the enrollment code is sent, as follows:

- 10 days, when sent to a postal address of record within the contiguous United States;
- 30 days, when sent to a postal address of record outside the contiguous United States;

- 10 minutes, when sent to a telephone of record (SMS or voice);
- 24 hours, when sent to an email address of record;
- 7 days if provided directly to the applicant during an in-person proofing session for authenticator binding at IAL2.

These validity periods are presented again in requirement IA-12 (5) g which presents the mandatory requirement for enrollment code confirmation for IAL2 remote identity proofing.

t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.

SUPPLEMENTAL GUIDANCE: The training requirement pertains to personnel performing the validation of identity evidence but does not specify training content. The CSP policies, guidelines, or requirements for validating identity evidence for identity proofing would be appropriate for the type of training intended by this requirement. Such content may include:

- the CSP's policy for types of evidence it collects and validates in order to meet the requirements of designated IALs;
- validation of security features for the types of identity evidence collected;
- detection of evidence alteration, falsification, or forgery for the types of identity evidence collected. Procedures for the validation of identity evidence information with issuing and authoritative sources.

This training may be accomplished through written training material, oral instruction, on-the-job training and mentoring, or other means. CSPs may perform some of the requirements for identity evidence validation through automated services and equipment. Therefore, personnel training would be based on the CSPs policies and procedures for the manual performance of evidence validation.

u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):

If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then…the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]. "

SUPPLEMENTAL GUIDANCE: In general, minors will not possess the types of evidence required to meet the CSP's minimum requirements for a given IAL. ICSPs that provide identity services to minors will need to determine and document the special considerations it applies to minors. Such special considerations may include the use of trusted referees and an expanded list of acceptable evidence types to include evidence a minor would likely possess, such as school IDs.

Requirements 'v' and 'w' apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also

apply to CSPs that optionally choose to collect biometric characteristics through in-person identity proofing and enrollment at IAL2.

v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

SUPPLEMENTAL GUIDANCE: Applicants may try to defraud the identity proofing process by using fake fingers or by applying non-natural materials - such as latex, silicon, or glue – to their fingers, faces, or other sources of biometrics. It is recommended that identity proofing operators be trained to recognize such practices and to examine all biometric sources used in the identity proofing for the presence of foreign materials.

It is recommended that the CSP documents and applies technologies and procedures which ensure that the proofing operator reviews the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

Requirements 'v' and 'w' apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2.

w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply.

SUPPLEMENTAL GUIDANCE: Applicants may try to defraud the identity proofing process by having another person present themselves for biometric collection. The risk of this happening is increased if the identity proofing process is not completed in a single session and during supervised remote identity proofing processes.

Documenting the technologies and procedures the CSP employs to ensure that biometric samples are taken from the applicant him/herself and not another person facilitates the assessment against this requirement.

x. The CSP SHALL support in-person or remote identity proofing, or both.

SUPPLEMENTAL GUIDANCE: IAL2 allows for remote or in-person identity proofing. IAL2 supports a wide range of acceptable identity proofing techniques in order to increase user adoption, decrease false negatives (legitimate applicants that cannot successfully complete identity proofing), and detect to the best extent possible the presentation of fraudulent identities by a malicious applicant.

Remote proofing presents challenges to achieving the desired outcomes described above that can be overcome through the use specific processes and technologies. Potential processes and controls that CSPs may employ to mitigate risks associated with remote identity proofing at IAL2 include:

1. A remote operator is present during at least part of the identity proofing session and

can provide positive confirmation that the requirements for IAL2 identity proofing are met. Employing real-time remote operators provides the capability for the identity proofing process to be completed in a single session and allows the remote operator to direct the applicant for proper presentation and examination of identity evidence and biometrics collection.

2. The CSP employs automated technologies and services (e.g., liveness detection, identity evidence verification and validation, and presentation attack detection, if applicable) which can ensure the requirements for IAL2 identity proofing are met and protect against spoofing attacks. This process also provides the capability for the identity proofing process to be completed in a single session.
3. The CSP employs an off-line operator to evaluate the evidence and images collected during a previous identity proofing process. In this scenario, the identity proofing process requires more than one session with the applicant and is not completed until the operator provides a positive confirmation that all requirements for IAL2 identity proofing are met.

y. The CSP SHALL collect the following from the applicant:
   1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR
   2. Two pieces of STRONG evidence; OR
   3. One piece of STRONG evidence plus two pieces of FAIR evidence

SUPPLEMENTAL GUIDANCE: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collecting the appropriate identity evidence, 2) confirming the evidence is genuine and authentic, and 3) confirming the data contained on the identity evidence is valid, current, and related to a real-life subject.

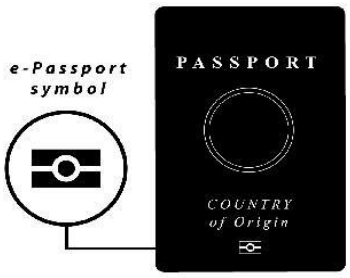
Figure 9 - Notional Strength of Evidence Types of this document presents notional strengths for types of evidence that may be presented for identity proofing purposes. Documenting the types and strengths of evidence the CSP collects for each proofing encounter demonstrates conformance for this requirement. (Also see IA-12 (3) l.)

Examples of methods and how they can be used to capture identity evidence images or extract data for validation include:

- Cameras to capture images of identity evidence for the purposes of evidence validation;
- Document scanner to capture images of identity evidence for the purpose of evidence validation; and
- Bar-code scanner to capture and extract information from standardized barcodes embedded on identity evidence.

High resolution images of at least 300 ppi are necessary for proper evidence examination and validation.

Figure 7 – Notional Strengths of Evidence Types

Type of Evidence	Strength	Notes
US Passport	Superior	Includes US Passport cards
Foreign e-Passport	Superior	
Personal Identity Verification (PIV) card	Superior	
Common Access card (CAC)	Superior	
Personal Identity Verification Interoperable (PIV-I) card	Superior	
Transportation Worker Identification Credential (TWIC)	Superior	
Permanent Resident Card	Superior	Issued on or after May 11, 2010
Native American Enhanced Tribal Card	Superior	

Type of Evidence	Strength	Notes
REAL ID cards	Strong+	Includes REAL ID driver’s licenses and ID cards. REAL ID cards have a star printed in the upper right-hand corner. Card and personal information must be validated with appropriate DMV or AAMVA.
Enhanced ID cards	Strong+	Includes Enhanced ID driver’s licenses and ID cards. Must be validated with appropriate DMV or AAMVA.
U.S. Uniformed Services Privilege and Identification Card (U.S. Military ID)	Strong+	Includes Uniformed Services Dependent ID Cards. Must be validated with appropriate military issuing source.
Permanent Resident Card	Strong	Issued Prior to May 11, 2010
Native American Tribal Photo Identification Card	Strong	
Driver's License or ID card (REAL ID non-compliant)	Strong	
School ID card	Fair	Includes facial image photograph
Utility account statement	Fair	
Credit/debit card and account statement	Fair	
Financial institution account statement	Fair	

Type of Evidence	Strength	Notes
US Social Security Card	Weak	
Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal	Weak	

z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see 'y' above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.

SUPPLEMENTAL GUIDANCE: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport, driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collect the appropriate identity evidence, 2) confirm the evidence is genuine and authentic, and 3) confirm the data contained on the identity evidence is valid, current, and related to a real-life subject.

Evidence validation for authenticity involves examining the evidence for:

- Confirmation of required information completeness and format for the identity evidence type.
- Detection of evidence tampering or the creation of counterfeit or fraudulent evidence.
- Confirmation of security features. See Figure 10 - Types of Identity Evidence Security Features to this document for types of commonly used security features for identity evidence.

Most of the capabilities to confirm security features on identity evidence are dependent upon physically viewing the evidence directly, tactile feel of the evidence, and viewing the evidence under specialized lighting or through the use of specialized equipment (see Figure 10 - Types of Identity Evidence Security Features). Therefore, the validation of evidence that may be submitted remotely for remote identity proofing methods is particularly challenging. For this reason, CSPs opting to provide remote identity proofing may find it most effective to use automated evidence validation products and services. If automated evidence validation solutions are not used, CSPs may choose to apply similar procedures for IAL2 remote proofing as are required for IAL3 supervised remote proofing. These procedures provide that a trained operator can remotely supervise the evidence collection process, require the applicant to turn or tilt evidence or apply lighting to be able to confirm security features on evidence that is presented for the identity proofing encounter in a recorded video or webcast. Alternatively, a CSP may use an automated interface for the capture

of identity evidence images that similarly can direct the applicant to turn, tilt or provide lighting on evidence presented for identity proofing purposes.

Figure 8 – Types of Identity Evidence Security Features

Security Feature (examination capability)	Description
Fine-line or Guilloche Pattern (visual)	Background pattern of continuous fine lines printed in wavy, overlapping pattern.
Ghost image (visual)	Half-tone reproduction of original image (e.g., facial image), may be printed behind printed data.
Overlapped data (visual)	Variable data (e.g., signature, seal, text) printed over another field such as facial image or seal.
Transparent image (visual)	See-through, window-like image feature (e.g., facial image) visible for both sides of the evidence.
Rainbow printing (visual)	Controlled color shifts of printed text in a continuous, linear fashion.
Holographic Images (visual, tilting)	Light field record of objects that will appear and change as view of evidence is tilted and turned. Most state-issued driver's licenses and IDs contain at least one holographic image.
Variable laser engraved images (visual, tilting)	Laser-engraved images at different angles so that image view changes with tilting angle of viewing evidence.
Iridescent Inks and Custom Foil Stamping (visual, tilting)	Custom designs and printing that will change color properties depending on the angle at which evidence is viewed.
Laser perforation (visual, light, tactile)	Perforated holes made by laser beam to form images. The images can be viewed under light source; image holes have tactile feel.
UV printing (visual, UV lighting)	A UV image or text that can only be viewed with special lighting. UV images may appear on the front or back of the evidence.

Security Feature (examination capability)	Description
Microprinting (visual, magnifier)	Microtext of static or variable data that can be confirmed when viewed under a magnifier. Requires magnification of at least 10X to view.
Laser embossing (tactile)	Use of laser to emboss image or text for tactile feel on only one side of the evidence.
Barcode (visual, barcode reader)	Machine readable, encoded data (typically personalized printed data) for 2-D barcode, readable with barcode reader.
UV printing (visual, UV lighting)	A UV image or text that can only be viewed with specialized lighting. UV images may appear on the front or back of a card.

The next step in identity evidence validation for authenticity and integrity is to verify the correctness of information from the identity evidence against the issuing source for the evidence or an authoritative source that has linkage to the issuing source. Results of these checks for authenticity and integrity should be recorded.

Figure 11 - Validating Identity Evidence lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein.

Figure 9 – Validating Identity Evidence

Strength	Method(s) Performed by the CSP
Unacceptable	• Evidence validation was not performed, or validation of the evidence failed.
Weak	• All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.

Strength	Method(s) Performed by the CSP
Fair	• Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), **OR** • The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** • The evidence has been confirmed as genuine by trained personnel, **OR** • The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.
Strong	• The evidence has been confirmed as genuine: o using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** o by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** o by confirmation of the integrity of cryptographic security features. • All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	• The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. • All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

aa. The CSP SHALL verify identity evidence as follows:

At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.

SUPPLEMENTAL GUIDANCE: The goal of identity verification is to confirm and establish a linkage between the validated evidence for the claimed identity and the real-life applicant presenting the evidence

The figure below shows IAL2 verification methods.

Figure 10 – Verification Methods and Strengths

Verification Strength	Verification Method	Description
Superior	Biometric Verification	Biometric comparison against biometric characteristics on the strongest piece(s) of evidence against live biometric capture for remote or in-person identity proofing. May be used for identity verification for FAIR, STRONG, and SUPERIOR strength.
Strong	In-Person Physical Verification	Physical comparison of applicant to facial-image photograph on strongest piece(s) of validated evidence. May be used for identity verification for FAIR and STRONG strength.
Strong	Remote Physical Verification	Physical comparison of applicant to facial-image photograph on strongest piece(s) of validated evidence. May be used for identity verification for FAIR and STRONG strength.

For IAL2 this linkage is achieved through a physical or biometric comparison of the facial image (i.e., photograph) on the strongest piece of evidence to the applicant or by a biometric comparison between information on the evidence and a biometric characteristic obtained from the applicant, most likely facial image.

Physical comparison is a comparison by a person (i.e., CSP-trained personnel) of the applicant to the photograph (i.e., facial image) on any of the strongest piece(s) of validated identity evidence collected. This comparison can be an in-person comparison for in-person identity proofing processes or may be conducted remotely for remote identity proofing. In both cases, the operator must perform a physical comparison of the applicant to the facial image photograph on the evidence. That is, the in-person proofing personnel will physically compare the facial image of the live applicant to the facial image photograph on the strongest piece of validated evidence. For remote physical comparison, the applicants' facial image may be captured by high resolution video or camera for physical comparison to the facial image photograph on the identity evidence.

For identity proofing verification, biometric comparison is an automated comparison of a biometric characteristic recorded on the strongest piece of identity evidence compared to the corresponding biometric characteristic of the applicant captured live during the identity proofing session.

Remote identity proofing requires the collection of both an image of the identity evidence and a live capture of the facial image of the applicant for physical or biometric comparison. The CSP must employ liveness and presentation attack detection capabilities to ensure that the applicant's facial image or other biometric characteristic used for comparison is "live" and not a spoofing or

presentation attack. Potential methods for remote identity proofing processes to mitigate such spoofing and presentation attacks are presented below.

- A remote operator is present during the identity proofing session (similar to supervised remote in-person proofing) and can conduct a real-time physical comparison between an image of the identity evidence and a live video of the applicant. In order to confirm the video stream is live and not pre-recorded, the Operator could direct the applicant to move their head in specific ways, or even ask the applicant a question. Once a positive confirmation is recorded from the operator, and all other requirements are met, the identity proofing can be completed in a single session.
- The CSP employs automated capabilities which are specifically designed to compare the image of the identity evidence with the applicant, and which also employ liveness detection technologies. Pending a positive confirmation from the automated comparison, and the satisfaction of all other requirements, the identity proofing can be completed in a single session.

The CSP employs liveness detection technology during the capture of the facial image, and an off-line operator performs the physical comparison of images captured during the identity proofing session. The identity proofing process requires more than one session with the applicant and is not completed until the operator provides a positive confirmation of the comparison and the other requirements are met.

bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m.

SUPPLEMENTAL GUIDANCE: See IA-5 m (1) – (12) for conformance criteria for the implementation and conformance assessment of requirements for the use of biometrics.

cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.

SUPPLEMENTAL GUIDANCE: identity verification is performed against the strongest piece of identity evidence submitted and validated. For IAL2 the strongest piece of evidence will always be either STRONG or SUPERIOR evidence. KBV (sometimes referred to as knowledge-based authentication) is only permitted as a verification method for evidence at the FAIR strength level; therefore, verification of FAIR evidence binding will never be required for IAL2.

dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJISSECPOL.

The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.

ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term "supervised remote identity proofing" has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. I f the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.

1. Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in IA-12(3)s.

   SUPPLEMENTAL GUIDANCE: Supervised remote identity proofing involves the use of a CSP-controlled station at a remote location that is connected to a trained operator at a central location. The goal of this arrangement is to permit identity proofing of individuals in remote locations where it is not practical for them to travel to the CSP for in-person identity proofing.

2. The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.

   SUPPLEMENTAL GUIDANCE: The integrity of supervised remote identity proofing depends upon the applicant being continuously present during the entire session. An applicant who steps away from an in-process session may do so to alter their biometric source or substitute a different person to complete the identity proofing process.

3. The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.

   SUPPLEMENTAL GUIDANCE: Having a trained operator supervise and participate in a remote identity proofing session reduces the opportunity for an applicant to defraud the process. As described in Appendix A Terms and Definitions, the operator is a person who has received specific training on enrollment and identity proofing procedures and the detection of potential fraud by an applicant.

4. The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.

   SUPPLEMENTAL GUIDANCE: The camera(s) a CSP employs to monitor the actions taken by a remote applicant during the identity proofing session should be positioned in such a way that the upper body, hands, and face of the applicant are always visible. Additionally, the components of the remote identity proofing station (including such things as keyboard, fingerprint capture device, signature pad, and scanner, as applicable) should be arranged such that all interactions with these devices is within the field of view.

5. The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.

   SUPPLEMENTAL GUIDANCE: Technologies exist that allow for the digital validation of identity evidence via electronic means (such as RFID to read the data off e-passports and chip readers for smartcards). The scanners and sensors employed to access these features should be integrated into the remote identity proofing stations in order to reduce the likelihood of being tampered with, removed, or replaced. To be integrated means the devices themselves are a component of the workstation (i.e., smartcard readers or fingerprint sensors built into a laptop) or the devices, and their connections, are secured in a protective case or locked box.

6. The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.

   SUPPLEMENTAL GUIDANCE: A comprehensive training program for supervised remote identity proofing operators may include some or all the following:

   - Purpose and objectives of the identity proofing and enrollment process, as employed by the CSP;
   - Supervised remote identity proofing process workflow;
   - Identity evidence validation processes;
   - Threats associated with the identity proofing process and how to detect potential fraud; and
   - System and process troubleshooting and problem resolution.

7. The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located.

   SUPPLEMENTAL GUIDANCE: For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall concourse.

8. The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.

   SUPPLEMENTAL GUIDANCE: Mutually authenticated protected channels employ approved cryptography to encrypt communications between

ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3), would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:

   - disabled individuals;
   - elderly individuals;
   - homeless individuals,
   - individuals with little or no access to online services or computing devices;
   - unbanked and individuals with little or no credit history;
   - victims of identity theft;
   - children under 18; and
   - immigrants.

In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.

1. If the CSP uses trusted referees, then…The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.

   SUPPLEMENTAL GUIDANCE: In instances where an individual cannot meet the identity evidence requirements specified in IA-12 (3) y – ee and IA-12 (5) b - i, the agency may use a trusted referee to assist in identity proofing the applicant. It is intended that CSPs using trusted referees for identity proofing and enrollment will document the procedures and controls in an applicable written policy or *practice statement* as described in IA-12 (3) h.

2. If the CSP uses trusted referees, then…The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing.

SUPPLEMENTAL GUIDANCE: Trusted referees, who participate in the identity proofing process on behalf of an applicant need to be identity proofed themselves to the same level as that of the applicant. If CSPs allows the use of Trusted Referees, its documented policies should state this requirement.

3. If the CSP uses trusted referees, then…The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.

   SUPPLEMENTAL GUIDANCE: In addition to proofing a Trusted Referee to the same (or greater) IAL as that of the applicant, CSPs will need to determine its process for proving a legitimate relationship to the applicant. The CSP should consider and document the types of evidence (i.e., power of attorney) it will accept to "bind" the relationship between Trusted Referee and an applicant. This minimum evidence may vary based on IAL.

Related Controls: None.

(5) IDENTITY PROOFING | ADDRESS CONFIRMATION

[Priority 2]

Control:

a. Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

DISCUSSION: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

b. The CSP SHALL confirm address of record.

SUPPLEMENTAL GUIDANCE: Valid records to confirm address are issuing source(s) or authoritative source(s). Ideally, the CSP will confirm an address of record through validation of the address contained on any supplied, valid piece of identity evidence. However, the CSP may confirm address of record by validating information supplied by the applicant that is not contained on any supplied piece of identity evidence. Postal addresses are preferred, however these guidelines support any type of address that can be validated against an issuing or authoritative source, whether physical or digital. Acceptable addresses of record include postal addresses, email addresses, and telephone numbers. The types of addresses of record a CSP accepts will determine, in part, the method it employs to validate them. For instance, postal addresses can be validated by confirming it against a piece of supplied, valid identity evidence. Email addresses may be confirmed by sending an email to the provided address.

c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).

Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.

SUPPLEMENTAL GUIDANCE: An address of record is a "validated and verified location (physical or digital) where an individual can receive communications using approved mechanisms." IAL2 requires confirming an applicant's address of record. This can be accomplished in two ways: 1) validation of the address contained on a valid piece of identity evidence, or 2) by employing a mechanism such as enrollment codes to validate an address not contained on a supplied piece of identity evidence.

Addresses that are supplied by an applicant, either verbally or on a non-valid piece of identity evidence, are not valid for confirming an applicant's address of record.

d. Note that IAL2-7 applies only to in-person proofing at IAL2.

If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code…SHALL be valid for a maximum of seven (7) days.

SUPPLEMENTAL GUIDANCE: Upon successful completion of the identity proofing process the CSP will typically register one or more authenticators to the subscribers' account or may optionally choose to bind an authenticator(s) at a later time. If the CSP chooses to use an enrollment code provided directly to the applicant to authenticate for such later binding, the validity period for the enrollment code is a maximum of seven days (see IA-12 (3) s).

Note that conformance criteria IA-12 (5) 'e' through 'i' apply to remote identity proofing processes at IAL2.

e. For remote identity proofing at IAL2:

The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.

SUPPLEMENTAL GUIDANCE: Enrollment codes used for IAL2 remote identity proofing may be sent to any confirmed address of record – postal, mobile phone number for SMS, or email addresses.

f. For remote identity proofing at IAL2:

The applicant SHALL present a valid enrollment code to complete the identity proofing process.

SUPPLEMENTAL GUIDANCE: Per IA-12 (5) e above, sending an enrollment code to a confirmed address of record, as captured during the identity proofing process, is required to complete the remote identity proofing process and provides additional confidence in the binding of that address to the applicant.

Valid enrollment codes mean that the correct enrollment code is submitted by the applicant within prescribed validity periods. Enrollment code validity periods depend on the type of address where the code is sent as shown in IA-12 (5) g below.

Information captured in the CSP's enrollment records or system logs facilitate assessment against this requirement. Ideally, this information would include details about the validity of the enrollment code (date and time applicant entered code; confirmation it was the correct code; and confirmation it was not expired).

g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.

   Enrollment codes shall have the following maximum validities:

   1. 10 days, when sent to a postal address of record within the contiguous United States;
   2. 30 days, when sent to a postal address of record outside the contiguous United States;
   3. 10 minutes, when sent to a telephone of record (SMS or voice);
   4. 24 hours, when sent to an email address of record.

SUPPLEMENTAL GUIDANCE: Enrollment codes sent to addresses of record are only valid for a limited amount of time, depending on the type of address of record to which they are sent. Applicants that present enrollment codes that are no longer valid (aka, expired) cannot use this code to complete their identity proofing process.

h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then…it SHALL be reset upon first use.

SUPPLEMENTAL GUIDANCE: Enrollment codes sent as an authentication factor for address confirmation may only be used once.

i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then…The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.

SUPPLEMENTAL GUIDANCE: For example, if the CSP sends an enrollment code to a phone number validated in records, a proofing notification may be sent to the postal address validated in records or obtained from validated and verified evidence, such as a driver's license.

Related Controls: IA-12.

INCIDENT RESPONSE (IR)

IR-1 POLICY AND PROCEDURES

[Existing] [Priority 2]

Control:

a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:

   1. Agency-level incident response policy that:

      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

   1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and

   2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

IR-2 INCIDENT RESPONSE TRAINING

[Existing] [Priority 2]

Control:

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
    1. Prior to assuming an incident response role or responsibility or acquiring system access;
    2. When required by system changes; and
    3. Annually thereafter; and
b. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-2 or AT-3.

Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8.

Control Enhancements:

(3) INCIDENT RESPONSE TRAINING | BREACH

[Priority 3]

Control:

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

Discussion: For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach.

IR-3 INCIDENT RESPONSE TESTING

[Priority 3]

Control:

Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests.

Discussion: Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related Controls: CP-3, CP-4, IR-2, IR-4, IR-8.

Control Enhancements:

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

[Priority 3]

Control:

Coordinate incident response testing with organizational elements responsible for related plans.

Discussion: Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

IR-4 INCIDENT HANDLING

[Existing] [Priority 2]

Control:

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Discussion: Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and

development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Related Controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

[Existing] [Priority 2]

Control:

Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

Discussion: Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis. Incident handling could be inherited from an upstream agency or could be part of a state-level process.

IR-5 INCIDENT MONITORING

[Existing] [Priority 2]

Control: Track and document incidents.

Discussion: Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-4 provides information on the types of incidents that are appropriate for monitoring.

Related Controls: AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

IR-6 INCIDENT REPORTING

[Priority 2]

Control:

a. Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery; and

b. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.

Discussion: The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

Related Controls: CM-6, CP-2, IR-4, IR-5, IR-8.

Control Enhancements:

(1) INCIDENT REPORTING | AUTOMATED REPORTING

[Existing] [Priority 2]

Control:

Report incidents using automated mechanisms.

Discussion: The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Related Controls: IR-7.

(3) INCIDENT REPORTING | SUPPLY CHAIN COORDINATION

[Priority 2]

Control:

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Related Controls: SR-8.

IR-7 INCIDENT RESPONSE ASSISTANCE

[Existing] [Priority 3]

Control:

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Discussion: Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

Related Controls: AT-2, AT-3, IR-4, IR-6, IR-8, SA-9.

Control Enhancements:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

[Priority 3]

Control:

Increase the availability of incident response information and support using automated mechanisms described in the discussion.

Discussion: Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

If the automated mechanisms include external assistance that will give unescorted physical or logical access to CJI, it is imperative to ensure that the appropriate controls/procedures (CJIS Security Addendum/Outsourcing Standard) are in place. Examples would include Cyber Incident Response Vendors (IT Security/Law Firms).

Related Controls: None.

IR-8 INCIDENT RESPONSE PLAN

[Existing] [Priority 2]

Control:

a. Develop an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by the organization's/agency's executive leadership annually; and
10. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO or CJIS WAN Official.

b. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities;

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to organizational personnel with incident handling responsibilities; and

e. Protect the incident response plan from unauthorized disclosure and modification.

Discussion: It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Related Controls: AC-2, CP-2, CP-4, IR-4, IR-7, PE-6, PL-2, SA-15, SI-12, SR-8.

Control Enhancements:

(1) INCIDENT RESPONSE PLAN | BREACHES

[Priority 2]

Control:

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
c. Identification of applicable privacy requirements.

Discussion: Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

Figure 11 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g., incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

MAINTENANCE (MA)

MA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with system maintenance responsibilities:
    1. Agency-level maintenance policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
c. Review and update the current maintenance:
    1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

MA-2 CONTROLLED MAINTENANCE

[Priority 3]

Control:

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction;

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records:

    1. Component name
    2. Component serial number
    3. Date/time of maintenance
    4. Maintenance performed
    5. Name(s) of entity performing maintenance including escort if required.

Discussion: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-11.

MA-3 MAINTENANCE TOOLS

[Priority 4]

Control:

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools prior to each use.

Discussion: Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer- used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Related Controls: MA-2, PE-16.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

[Priority 4]

Control:

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Discussion: Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

[Priority 4]

Control:

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Discussion: If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls: SI-3.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

[Priority 4]

Control:

Prevent the removal of maintenance equipment containing organizational information by:

a. Verifying that there is no organizational information contained on the equipment;
b. Sanitizing or destroying the equipment;
c. Retaining the equipment within the facility; or
d. Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility.

Discussion: Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related Controls: MP-6.

MA-4 NONLOCAL MAINTENANCE

[Priority 3]

Control:

a. Approve and monitor nonlocal maintenance and diagnostic activities;
b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed.

Discussion: Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls.

Related Controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

MA-5 MAINTENANCE PERSONNEL

[Priority 3]

Control:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Discussion: Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

MA-6 TIMELY MAINTENANCE

[Priority 3]

Control:

Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.

Discussion: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related Controls: CM-8, CP-2, CP-7, RA-7, SA-15, SR-2, SR-3.

MEDIA PROTECTION (MP)

Documented and implemented media protection policies and procedures ensure that access to digital and non-digital media in all forms is restricted to authorized individuals using authorized methods and processes.

MP-1 POLICY AND PROCEDURES

[Existing] [Priority 2]

Control:

a. Develop, document, and disseminate to authorized individuals:
    1. Agency-level media protection policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and
c. Review and update the current media protection:
    1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and
    2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.

Discussion: Media protection policy and procedures address the controls in the MP family that are implemented within systems and agencies. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the agency level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of agencies. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an agency policy or procedure.

Related Controls: PS-8, SI-12.

MP-2 MEDIA ACCESS

[Existing] [Priority 2]

Control:

Restrict access to digital and non-digital media to authorized individuals.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to hard copies of case file information stored in a locked filing cabinet is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

Related Controls: AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SI-12.

~~MP-3 MEDIA MARKING~~

~~[Priority 3]~~

~~Control:~~

~~a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and~~

~~b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations or controlled areas.~~

~~Discussion: Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information (CUI) is defined by the National Archives and Records Administration (NARA) along with the appropriate safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002]. Security markings are generally not required for media that contains information determined by agencies to be in the public domain or to be publicly releasable. Some agencies may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Executive Order 13556 mandates the marking of CUI. The following categories of CJI fall under the designated NARA categories which direct marking as indicated.~~

~~1. Biometric Data – data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data. NARA CUI Category: Sensitive Personally Identifiable Information. NARA Banner Marking: CUI~~

2. Identity History Data – textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual. NARA CUI Category: Criminal History Records Information. NARA Banner Marking: CUI//SP-CHRI

3. Biographic Data – information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case. NARA CUI Category: General Law Enforcement. NARA Banner Marking: CUI

4. Property Data – information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII). NARA CUI Category: General Law Enforcement. NARA Banner Marking: CUI

5. Case/Incident History – information about the history of criminal incidents. NARA CUI Category: General Law Enforcement. NARA Banner Marking: CUI

[32 CFR 2002] states the CUI Program prohibits using markings or practices not included in this part or the CUI Registry. If legacy markings remain on information, the legacy markings are void and no longer indicate that the information is protected or that it is or qualifies as CUI.

Related Controls: CP-9, MP-5, SI-12.

MP-4 MEDIA STORAGE

[Existing] [Priority 2]

Control:

a. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on agencies, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related Controls: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SI-12.

MP-5 MEDIA TRANSPORT

[Existing] [Priority 2]

Control:

a. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in SC-13 and SC-28 of this Policy. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel;

b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which agencies provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the agency. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Agencies establish documentation requirements for activities associated with the transport of system media in accordance with agency assessments of risk. Agencies maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related Controls: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28.

MP-6 MEDIA SANITIZATION

[Existing] [Priority 2]

Control:

a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of

when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Discussion: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Agencies determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.

Agencies use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on agencies or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Related Controls: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, SI-12, SR-11.

MP-7 MEDIA USE

[Existing] [Priority 2]

Control:

a. Restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls (examples below); and

b. Prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information; and

c. Prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.

Examples of technical controls: port disabling, access control lists (ACL), security groups, group policy objects (GPO), mobile device management (MDM).

Example of physical control: locked server cage, disconnect CD-ROM drive in PC, remove USB port.

Example of administrative controls: the agency's electronic media policy defining how flash drives are to be used within the agency rules of behavior.

Discussion: System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Agencies use technical and nontechnical controls to restrict the use of system media. Agencies may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or write to such devices. Agencies may also limit the use of portable storage devices to only approved devices, including devices provided by the agency, devices provided by other approved agencies, and devices that are not personally owned. Finally, agencies may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing agencies to assign responsibility for addressing known vulnerabilities in the devices.

Related Controls: AC-19, AC-20, PL-4.

Figure 12 – A Local Police Department's Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor's vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentially of the police department's data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor's vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

PE-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with physical and environmental protection responsibilities:
   1. Agency-level physical and environmental protection policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:
   1. Policy annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI; and
   2. Procedures annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.

Discussion: Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AT-3, PS-8, SI-12.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

[Existing] [Priority 2]

Control:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals annually and when personnel changes occur; and

d. Remove individuals from the facility access list when access is no longer required.

Discussion: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

Related Controls: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PS-3, PS-4, PS-5, PS-6.

PE-3 PHYSICAL ACCESS CONTROL

[Existing] [Priority 2]

Control:

a. Enforce physical access authorizations by:

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using agency-implemented procedures and controls;

b. Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas;

c. Control access to areas within the facility designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers;

d. Escort visitors and control visitor activity in all physically secure locations;

e. Secure keys, combinations, and other physical access devices;

f. Inventory all agency-issued physical access devices annually; and

g. Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

h. If the above conditions cannot be met refer to the requirements listed in PE-17.

Discussion: Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas.

Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Related Controls: AT-3, AU-2, AU-6, AU-9, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

PE-4 ACCESS CONTROL FOR TRANSMISSION

[Existing] [Priority 2]

Control:

Control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls.

Discussion: Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related Controls: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

[Existing] [Priority 3]

Control:

Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.

Discussion: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored

by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related Controls: PE-2, PE-3, PE-4.

PE-6 MONITORING PHYSICAL ACCESS

[Existing] [Priority 2]

Control:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
b. Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.

Discussion: Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Related Controls: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Control Enhancements:

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT

[Existing] [Priority 2]

Control:

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Discussion: Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and

broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Related Controls: None.

PE-8 VISITOR ACCESS RECORDS

[Priority 4]

Control:

a. Maintain visitor access records to the facility where the system resides for one (1) year;
b. Review visitor access records quarterly; and
c. Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.

Discussion: Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Related Controls: PE-2, PE-3, PE-6.

Control Enhancements:

(3) VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Priority 4]

Control:

Limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

Note: Access to visitor access records is restricted to authorized agency personnel.

Discussion: Organizations may have requirements that specify the contents of visitor access records. Limiting personally identifiable information in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3, SA-8.

PE-9 POWER EQUIPMENT AND CABLING

[Priority 2]

Control:

Protect power equipment and power cabling for the system from damage and destruction.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls: PE-4.

PE-10 EMERGENCY SHUTOFF

[Priority 2]

Control:

a. Provide the capability of shutting off power to all information systems in emergency situations;

b. Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related Controls: PE-15.

PE-11 EMERGENCY POWER

[Priority 2]

Control:

Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from

unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls: AT-3, CP-2, CP-7.

PE-12 EMERGENCY LIGHTING

[Priority 2]

Control:

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

Related Controls: CP-2, CP-7.

PE-13 FIRE PROTECTION

[Priority 2]

Control:

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

Related Controls: AT-3.

Control Enhancements:

(1) FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

[Priority 2]

Control:

Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

PE-14 ENVIRONMENTAL CONTROLS

[Priority 2]

Control:

a. Maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels; and

b. Monitor environmental control levels continuously.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Related Controls: AT-3, CP-2.

PE-15 WATER DAMAGE PROTECTION

[Priority 2]

Control:

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms,

and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related Controls: AT-3, PE-10.

PE-16 DELIVERY AND REMOVAL

[Existing] [Priority 3]

Control:

a. Authorize and control information system-related components entering and exiting the facility; and

b. Maintain records of the system components.

Discussion: Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Related Controls: CM-3, CM-8, MA-2, MA-3, MP-5, SR-2, SR-3, SR-6.

PE-17 ALTERNATE WORK SITE

[Existing] [Priority 3]

Control:

a. Determine and document all alternate facilities or locations allowed for use by employees;

b. Employ the following controls at alternate work sites:

    1. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.

    2. Lock the area, room, or storage container when unattended.

    3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.

    4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Discussion: Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of

organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related Controls: AC-17, AC-18, CP-7.

PLANNING (PL)

PL-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with planning responsibilities:

   1. Agency-level planning policy that:

      (c) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (d) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

   1. Policy annually and following; any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI and

   2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

[Priority 2]

Control:

a. Develop security and privacy plans for the system that:
   1. Are consistent with the organization's enterprise architecture;
   2. Explicitly define the constituent system components;
   3. Describe the operational context of the system in terms of mission and business processes;
   4. Identify the individuals that fulfill system roles and responsibilities;
   5. Identify the information types processed, stored, and transmitted by the system;
   6. Provide the security categorization of the system, including supporting rationale;
   7. Describe any specific threats to the system that are of concern to the organization;
   8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
   9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
   10. Provide an overview of the security and privacy requirements for the system;
   11. Identify any relevant control baselines or overlays, if applicable;
   12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
   13. Include risk determinations for security and privacy architecture and design decisions;
   14. Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities; and
   15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities;

c. Review the system security and privacy plans at least annually or when required due to system changes or modifications;

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Discussion: System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). The CJISSECPOL describes the different types of requirements that are relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-8, PL-10, PL-11, RA-3, RA-9, SA-5, SA-22, SI-12, SR-2.

PL-4 RULES OF BEHAVIOR

[Priority 3]

Control:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior at least annually; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated.

Discussion: Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

Related Controls: AC-2, AC-6, AC-8, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

Control Enhancements:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS

[Priority 3]

Control:

Include in the rules of behavior, restrictions on:

a. Use of social media, social networking sites, and external sites/applications;

b. Posting organizational information on public websites; and

c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Discussion: Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

Related Controls: AC-22.

PL-8 SECURITY AND PRIVACY ARCHITECTURES

[Priority 2]

Control:

a. Develop security and privacy architectures for the system that:
    1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
    2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
    3. Describe how the architectures are integrated into and support the enterprise architecture; and
    4. Describe any assumptions about, and dependencies on, external systems and services;
b. Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture; and
c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

Discussion: The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

[SP 800-160-1] provides guidance on the use of security architectures as part of the system development life cycle process. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the

proposed architecture in the RFP responses to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

Related Controls: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, RA-9, SA-3, SA-5, SA-8, SC-7.

PL-9 CENTRAL MANAGEMENT

[Priority 4]

Control:

The CJISSECPOL is centrally managed by the FBI CJIS ISO.

Discussion: Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.

As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-

17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.

Related Controls: PL-8.

PL-10 BASELINE SELECTION

[Priority 3]

Control:

Select a control baseline for the system.

Discussion: Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in [SP 800-53B]. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in [SP 800-53B] are based on the requirements from [FISMA] and [PRIVACT]. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. [CNSSI 1253] provides guidance on control baselines for national security systems.

Related Controls: PL-2, PL-11, RA-2, RA-3, SA-8.

PL-11 BASELINE TAILORING

[Priority 3]

Control:

Tailor the selected control baseline by applying specified tailoring actions.

Discussion: The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans

that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in [SP 800-53B]. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in [SP 800-53B] can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in [SP 800-53B] in accordance with the security and privacy requirements from [FISMA], [PRIVACT], and [OMB A-130]. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in [SP 800-53B] to specialize or customize the controls that represent the specific needs and concerns of those entities.

Related Controls: PL-10, RA-2, RA-3, RA-9, SA-8.

PERSONNEL SECURITY (PS)

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI. Regardless of the implementation model – physical data center, virtual cloud solution, or a hybrid model – unescorted access to unencrypted CJI must be determined by the criminal and noncriminal justice agency taking into consideration if those individuals have unescorted logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI.

PS-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with personnel security responsibilities:
   1. Agency-level personnel security policy that:
      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:
   1. Policy annually and following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures annually and following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Discussion: Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for

mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

PS-2 POSITION RISK DESIGNATION

[Priority 2]

Control:

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations as required.

Discussion: Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems.

Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for federal organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

Related Controls: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SI-12.

PS-3 PERSONNEL SCREENING

[Existing] [Priority 2]

Control:

a. Screen individuals prior to authorizing access to the information system;

   1. To properly screen, state of residency and national fingerprint-based record checks shall be conducted. National fingerprint-based record checks must be conducted pursuant to an FBI approved authority such as a federal statute or a state statute approved pursuant to Public Law 92-544. If the person resides in a different state than that of the assigned agency, the agency shall also conduct state (of the agency) record checks. When appropriate, the screening shall be consistent with:

      a. 5 CFR 731.106; and/or

      b. Office of Personnel Management policy, regulations, and guidance; and/or

      c. agency policy, regulations, and guidance.

      Agencies authorized to bypass state repositories in compliance with federal law must only conduct a national fingerprint-based record check.

      Agencies without approved statutory authority authorizing or requiring civil fingerprint-based record checks on personnel with access to CHRI are exempt from this requirement until such time as appropriate statutory authority is obtained to conduct such record checks.

   2. All requests for access shall be made as specified by the CSO, Authorized Recipient Official, or IA Official. The CSO/designee, Authorized Recipient Official/designee, or IA Official is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency. All Authorized Recipient designees shall be employed by the Authorized Recipient Agency.

   3. If a criminal history record of any kind exists, access to CJI shall not be granted until the CSO/designee, Authorized Recipient Official/designee, or IA Official reviews the matter to determine if access is appropriate.

      a. If a felony conviction of any kind exists, the agency shall deny access to CJI. However, the requesting agency may ask for a review by the CSO/designee, Authorized Recipient Official/designee, or IA Official in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

      b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO/designee, Authorized Recipient Official/designee, or IA Official, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The requesting agency may request the CSO/designee, Authorized Recipient Official/designee, or IA Official review a denial of access determination.

      c. If a criminal history record of any kind is found on a contractor, the CA shall be formally notified of continuing fitness determination and system access shall be delayed pending review of the criminal history record information. The CA shall in turn notify the contractor's security officer.

   4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO/designee, Authorized Recipient Official/designee, or IA Official shall review the

matter to determine if access to CJI is appropriate.

5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO/designee, Authorized Recipient Official/designee, or IA Official. This does not implicitly grant hiring/firing authority with the CSA, Authorized Recipient, or IA Official only the authority to grant access to CJI. For offenses other than felonies, the CSO/designee, Authorized Recipient Official/designee, or IA Official has the latitude to delegate continued access determinations.
6. If the CSO/designee, Authorized Recipient Official/designee, or IA Official determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The criminal and non-criminal justice agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO/designee, Authorized Recipient Official/designee, or IA Official.

   and

b. Recommend rescreening individuals in accordance with PS-3(a)(1) above. The authority authorized for the national fingerprint-based background check must also authorize the rescreening.

Discussion: Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks.

Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related Controls: AC-2, IA-4, MA-5, PE-2, PS-2, PS-6, PS-7.

PS-4 PERSONNEL TERMINATION

[Priority 2]

Control:

Upon termination of individual employment:

a. Disable system access within twenty-four (24) hours;
b. Terminate or revoke any authenticators and credentials associated with the individual;
c. Conduct exit interviews that include a discussion of non-disclosure of CJI and PII;
d. Retrieve all security-related organizational system-related property; and
e. Retain access to organizational information and systems formerly controlled by

terminated individual.

Discussion: System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

Related Controls: AC-2, IA-4, PE-2, PS-6, PS-7.

PS-5 PERSONNEL TRANSFER

[Priority 3]

Control:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate appropriate actions such as closing and establishing accounts and changing system access authorizations within twenty-four (24) hours;

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, and organizational personnel with account management responsibilities prior to personnel transfer.

Discussion: Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted.
Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Related Controls: AC-2, IA-4, PE-2, PS-4, PS-7.

PS-6 ACCESS AGREEMENTS

[Priority 4]

Control:

a. Develop and document access agreements for organizational systems;
b. Review and update the access agreements at least annually; and
c. Verify that individuals requiring access to organizational information and systems:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or when signatories change.

Discussion: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SI-12.

PS-7 EXTERNAL PERSONNEL SECURITY

[Existing] [Priority 2]

Control:

a. Establish personnel security requirements, including security roles and responsibilities for external providers;
b. Require external providers to comply with personnel security policies and procedures established by the organization;
c. Document personnel security requirements;
d. Require external providers to notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, or organizational personnel with account management responsibilities of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within twenty-four (24) hours; and
e. Monitor provider compliance with personnel security requirements.

Discussion: External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or

system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Related Controls: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA- 9.

PS-8 PERSONNEL SANCTIONS

[Priority 4]

Control:

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and
b. Notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, or organizational personnel with account management responsibilities within twenty-four (24) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Discussion: Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies.
Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Related Controls: All XX-1 Controls, PL-4, PS-6.

PS-9 POSITION DESCRIPTIONS

[Priority 4]

Control:

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Discussion: Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Figure 13 – Personnel Security Use Cases

Use Case 1 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated policies. The police department re-evaluated each person's suitability for access to CJI every five years.

Use Case 2 – Infrastructure as a Service (IaaS) Cloud Service Implementation

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure – as defined in Appendix G.3.

A local agency implements an IaaS solution in a cloud environment leveraging an agency-implemented secure virtual private cloud which has been identified to meet the appropriate security controls in the CJIS Security Policy. The agency maintains sole access to the encryption keys. In this scenario, cloud service provider personnel have no logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI; therefore, no fingerprint-based background checks are required to comply with the CJIS Security Policy. Refer to Appendix G.3 Cloud Computing for additional implementation guidance.

Use Case 3 – Platform as a Service (PaaS) Cloud Service Implementation

This model provides the consumer the capability to deploy consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.*

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model, the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage – as defined in Appendix G.3.

An agency utilizes a cloud service solution involving PaaS to write code, build, or develop a new application. There is no CJI associated with the code development. Although cloud service personnel provide support for the platform (i.e., hardware and software maintenance), no CJI is being accessed during development. The cloud service provider has no unescorted logical or physical access to any information system and no ability, right, or privilege to view, modify, or make use of unencrypted CJI. Refer to Appendix G.3 Cloud Computing for additional implementation guidance.

Use Case 4 – Software as a Service (SaaS) Cloud Service Implementation

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model, it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings – as defined in Appendix G.3

An agency utilizes a SaaS provider for their records management system (RMS). The SaaS provider hosts their solution on a cloud provider. The SaaS provider directly supports the agency for updates and management of the solution and has unescorted logical or physical access to the information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI within the RMS. The cloud provider, however, does not have unescorted logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI as the SaaS provider maintains the encryption keys. In this scenario, the agency would be required to comply with Section 5.12 for employees of the SaaS provider with access to CJI but would not need to do so for employees of the cloud provider used by the SaaS provider. Refer to Appendix G.3 Cloud Computing for additional implementation guidance.

RISK ASSESSMENT (RA)

RA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with risk assessment responsibilities:
    1. Agency Level risk assessment policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;
b. Designate organizational personnel with security and privacy responsibilities to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
c. Review and update the current risk assessment:
    1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

RA-2 SECURITY CATEGORIZATION

[Priority 2]

Control:

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Discussion: Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. The FBI CJIS Advisory Policy Board (APB) has assigned a security categorization of "moderate" for CJI and systems that process, store, and transmit CJI.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

Related Controls: CM-8, MP-4, PL-2, PL-10, PL-11, RA-3, RA-5, RA-7, SA-8, SC-7, SI-12.

RA-3 RISK ASSESSMENT

[Priority 2]

Control:

a. Conduct a risk assessment, including:
    1. Identifying threats to and vulnerabilities in the system;
    2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
    3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in a risk assessment report;
d. Review risk assessment results at least quarterly;
e. Disseminate risk assessment results to organizational personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities; and
f. Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Discussion: Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

Related Controls: CA-3, CA-6, CM-4, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PL-2, PL-10, PL-11, RA-2, RA-5, RA-7, SA-8, SA-9, SI-12.

RA-5 VULNERABILITY MONITORING AND SCANNING

[Priority 1]

Control:

a. Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities within the number of days listed;
    - Critical–15 days

- High–30 days
- Medium–60 days
- Low–90 days; and

e. Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Discussion: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use

public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as "bug bounties") to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization's needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Related Controls: CA-2, CA-7, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SI-2, SI-3, SI-4, SI-7, SR-11.

Control Enhancements:

(2) VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED

[Priority 1]

Control:

Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported.

Discussion: Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Related Controls: SI-5.

(5) VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS

[Priority 1]

Control:

Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access.

Discussion: In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Related Controls: None.

(11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM

[Priority 1]

Control:

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Discussion: The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non- disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

Related Controls: None.

RA-7 RISK RESPONSE

[Priority 2]

Control:

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Discussion: Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed.

However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

Related Controls: CA-5, RA-2, RA-3, SR-2.

RA-9 CRITICALITY ANALYSIS

[Priority 2]

Control:

Identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.

Discussion: Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of

a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Related Controls: CP-2, PL-2, PL-8, PL-11, RA-2, SA-8, SA-15, SR-5.

SYSTEM AND SERVICES ACQUISITION (SA)

SA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to: organizational personnel with system and services acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities:

   1. Agency/Entity information systems and services acquisition policy for systems used to process, store, or transmit CJI that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate organizational personnel with information security responsibilities and organizational personnel with system and services acquisition responsibilities to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

   1. Policy following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and

   2. Procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events

that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

SA-2 ALLOCATION OF RESOURCES

[Priority 2]

Control:

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

Discussion: Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

Related Controls: SA-9, SR-3, SR-5.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

[Priority 2]

Control:

a. Acquire, develop, and manage the system using an agency documented system development lifecycle process that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Discussion: A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of

information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

Related Controls: PL-8, SA-4, SA-5, SA-8, SA-11, SA-15, SA-22, SR-3, SR-5,

SA-4 ACQUISITION PROCESS

[Priority 2]

Control:

Include the following requirements, descriptions, and criteria, explicitly or by reference, using agency defined contract language in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

Discussion: Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities.

Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

Related Controls: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SR-3, SR-5.

Control Enhancements:

(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF CONTROLS

[Priority 2]

Control:

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Discussion: Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

Related Controls: None.

(2) ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS

[Priority 2]

Control:

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design and a project plan that addresses sufficient detail to permit analysis and testing of the controls.

Discussion: Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Related Controls: None.

(9) ACQUISITION PROCESS | FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE

[Priority 2]

Control:

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Discussion: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring

system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

Related Controls: CM-7, SA-9.

(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

[Priority 2]

Control:

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

Discussion: Products on the FIPS 201-approved products list meet requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multi-factor authentication in systems and organizations.

Related Controls: IA-2, IA-8.

SA-5 SYSTEM DOCUMENTATION

[Priority 3]

Control:

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security and privacy functions and mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;
b. Obtain or develop user documentation for the system, system component, or system service that describes:
    1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
    3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document steps to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent by contacting manufacturers, suppliers, or developers and conducting web-based searches in response; and

d. Distribute documentation to organizational personnel with system and services responsibilities.

Discussion: System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system.

Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SI-12, SR-3.

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

[Priority 2]

Control:

Apply agency documented systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components.

Discussion: Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-3). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system

security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions.

System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

Related Controls: PL-8, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SC-2, SC-39, SR-2, SR-3, SR- 5.

Control Enhancements:

(33) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZATION

[Priority 2]

Control:

Implement the privacy principle of minimization using only the Personally Identifiable Information necessary to perform system engineering.

Discussion: The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

Related Controls: PE-8, SI-12.

SA-9 EXTERNAL SYSTEM SERVICES

[Priority 2]

Control:

a. Require that providers of external system services comply with organizational security and privacy requirements and employ system and services acquisition security controls in accordance with the CJISSECPOL including the following agreements when applicable:

1. Management control agreement: A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA stipulating management control of the criminal justice function remains solely with the CJA. An example of an NCJA (government) is a city information technology (IT) department. An example of an MCA is provided in Appendix D.2.
2. Security Addendum: The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7), which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJISSECPOL, provides for sanctions, and contains such other provisions as the Attorney General may require.

   Private contractors designated to:

   a. Perform criminal justice functions for a CJA; or
   b. Perform criminal justice dispatching functions or data processing/information services for a NCJA (government), shall be eligible for access to CJI pursuant to an agreement which specifically identifies the private contractor's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA/NCJA and the private contractor shall incorporate the CJISSECPOL.

   Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page (page H- 8), compliance with all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H (pages H-6 and 7). Modifications to the CJIS Security Addendum shall be enacted only by the FBI.
3. Outsourcing Standards for Channelers: Channelers designated to request civil fingerprint-based background checks on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and

Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.

4. Outsourcing Standards for Non-Channelers: Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis:

1. All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.
2. At a minimum, triennially audit all external service providers which have access to the information system in order to ensure compliance with applicable statutes, regulations, and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of external service providers facilities.
4. Have the authority, on behalf of another CSA, to conduct a CJISSECPOL compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: Compliance audit requirements are outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channeling related to outsourcing noncriminal justice administrative functions.

Discussion: External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements.

Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related Controls: AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR- 5.

Control Enhancements:

(2) EXTERNAL SYSTEM SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES

[Priority 2]

Control:

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: any system with a local, network, or remote connection to an agency information system.

Discussion: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related Controls: CM-6, CM-7.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

[Priority 2]

Control:

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service during design, development, implementation, operation, and disposal;

b. Document, manage, and control the integrity of changes to security configuration, network diagrams, and system components (hardware, software, firmware) by implementing access restrictions such as least privilege for changes;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to the individual(s) with information security responsibilities and an individual(s) with system and services acquisition responsibilities.

Discussion: Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls.

Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation.

Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

Related Controls: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-5, SR-6.

SA-11 DEVELOPER TESTING AND EVALUATION

[Priority 2]

Control:

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy control assessments;

b. Perform system and regression testing/evaluation at a level of comprehensive testing;

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

Discussion: Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws.

Testing custom software applications may require approaches, such as manual code review, security architecture review, and penetration testing, as well as and static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

Related Controls: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SI-2, SR-5, SR-6.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

[Priority 3]

Control:

a. Require the developer of the system, system component, or system service to follow a documented development process that:

   1. Explicitly addresses security and privacy requirements;

   2. Identifies the standards and tools used in the development process;

3. Documents the specific tool options and tool configurations used in the development process; and
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy security and privacy requirements during design, development, implementation, operation, and disposal.

Discussion: Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Related Controls: MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-5, SR-6.

Control Enhancements:

(1) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS |CRITICALITY ANALYSIS

[Priority 3]

Control:

Require the developer of the system, system component, or system service to perform a criticality analysis:

a. At the following decision points in the system development life cycle: design, development, implementation, and operational; and

b. At the following level of rigor: comprehensive testing.

Discussion: Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, source code, and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. High value assets can be moderate- or high-impact systems due to heightened adversarial interest or potential adverse effects on the federal enterprise.

Developer input is especially important when organizations conduct supply chain criticality analyses.

Related Controls: RA-9.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

[Priority 2]

Control:

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support.

Discussion: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components.

Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation.

Related Controls: PL-2, SA-3.

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the requirements for protecting systems and communications infrastructures.

SC-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with system and communications protection responsibilities:
    1. Agency-level system and communications protection policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;
b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and
c. Review and update the current system and communications protection:
    1. Policy annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may

precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

[Existing] [Priority 2]

Control:

Separate user functionality, including user interface services, from system management functionality.

Discussion: System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8.

Related Controls: AC-6, SA-4, SA-8, SC-7, SC-22, SC-39.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

[Existing] [Priority 2]

Control:

Prevent unauthorized and unintended information transfer via shared system resources.

Discussion: Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are

manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Related Controls: AC-3, AC-4, SA-8.

SC-5 DENIAL-OF-SERVICE PROTECTION

[Priority 2]

Control:

a. Protect against or limit the effects of the following types of denial-of-service events: distributed denial of service, DNS Denial of Service, etc.; and

b. Employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices.

Discussion: Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

Related Controls: CP-2, IR-4, SC-7.

SC-7 BOUNDARY PROTECTION

[Existing] [Priority 1]

Control:

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Discussion: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. [SP 800-

189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

Related Controls: AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, SA-8, SC-5.

Control Enhancements:

(3) BOUNDARY PROTECTION | ACCESS POINTS

[Priority 1]

Control:

Limit the number of external network connections to the system.

Discussion: Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. A Trusted Internet Connection (TIC) initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

Related Controls: None.

(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

[Priority 1]

Control:

a. Implement a managed interface for each external telecommunication service;

b. Establish a traffic flow policy for each managed interface;

c. Protect the confidentiality and integrity of the information being transmitted across each interface;

d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

e. Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while removing exceptions that are no longer supported by an explicit mission or business need;

f. Prevent unauthorized exchange of control plane traffic with external networks;

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

Discussion: External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

Related Controls: AC-3, SC-8, SC-20, SC-21, SC-22.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION

[Priority 1]

Control:

Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJI.

Discussion: Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Related Controls: None.

(7) BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES

[Priority 1]

Control:

Prevent split tunneling for remote devices connecting to organizational systems.

Discussion: Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

Related Controls: None.

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

[Existing] [Priority 1]

Control:

Route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces.

Discussion: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for "man-in-the-middle" attacks (depending on the implementation).

Related Controls: AC-3.

(24) BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION

[Priority 1]

Control:

For systems that process personally identifiable information:

a. Apply the following processing rules to data elements of personally identifiable information: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;

b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;

c. Document each processing exception; and

d. Review and remove exceptions that are no longer supported.

Discussion: Managing the processing of personally identifiable information is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.

Related Controls: None.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

[Existing] [Priority 2]

Control:

Protect the confidentiality and integrity of transmitted information.

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

Discussion: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques. Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls. The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content–similar to the AU controls), data usage/indexing metrics, and diagnostic/syslog data.

Related Controls: AC-17, AC-18, IA-3, IA-8, MA-4, PE-4, SA-4, SA-8, SC-7, SC-20, SC-23, SC-28.

Control Enhancements:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION

[Existing] [Priority 2]

Control:

Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access to CJI during transmission.

Discussion: Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to

protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Related Controls: SC-12, SC-13.

SC-10 NETWORK DISCONNECT

[Priority 3]

Control:

Terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity.

NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) and used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

Discussion: Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Related Controls: AC-17, SC-23.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

[Existing] [Priority 2]

Control:

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency.

Discussion: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. [NIST CMVP] and [NIST CAVP] provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

Related Controls: AC-17, AU-9, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-12, SC-13, SC-17, SC-20, SI-3, SI-7.

SC-13 CRYPTOGRAPHIC PROTECTION

[Existing] [Priority 2]

Control:

a. Determine the use of encryption for CJI in-transit when outside a physically secure location; and

b. Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliancy can be used in the interim until certification is complete. FIPS 140-2 certificates will not be acceptable after September 21, 2026.

Discussion: Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SI-3, SI-7.

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

[Priority 2]

Control:

a. Prohibit remote activation of collaborative computing devices and applications; and

b. Provide an explicit indication of use to users physically present at the devices.

Discussion: Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

Related Controls: AC-21.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

[Existing] [Priority 2]

Control:

a. Issue public key certificates under an agency-level certificate authority or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Discussion: Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

Related Controls: IA-5, SC-12.

SC-18 MOBILE CODE

[Priority 3]

Control:

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

Discussion: Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Related Controls: AU-2, AU-12, CM-2, CM-6, SI-3.

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

[Priority 2]

Control:

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Discussion: Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Related Controls: SC-8, SC-12, SC-13, SC-21, SC-22.

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

[Priority 2]

Control:

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Discussion: Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and

address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

Related Controls: SC-20, SC-22.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

[Priority 2]

Control:

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Discussion: Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

Related Controls: SC-2, SC-20, SC-21.

SC-23 SESSION AUTHENTICITY

[Priority 2]

Control:

Protect the authenticity of communications sessions.

Discussion: Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions.

Related Controls: SC-8, SC-10.

SC-28 PROTECTION OF INFORMATION AT REST

[Existing] [Priority 2]

Control:

Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States–federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (e.g., the Preventing and Combating Serious Crime agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Discussion: Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage. The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content–similar to the AU controls), data usage/indexing metrics, and diagnostic/syslog data.

Related Controls: AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SI-3, SI-7, SI-16.

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

[Existing] [Priority 2]

Control:

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI.

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

Related Controls: AC-19, SC-12, SC-13.

SC-39 PROCESS ISOLATION

[Existing] [Priority 2]

Control:

Maintain a separate execution domain for each executing system process.

Discussion: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

Related Controls: AC-3, AC-4, AC-6, SA-8, SC-2, SI-16.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department's Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state's CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

SYSTEM AND INFORMATION INTEGRITY (SI)

SI-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:
   1. Agency-level system and information integrity policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:
   1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
   2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

SI-2 FLAW REMEDIATION

[Existing] [Priority 1]

Control:

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;

- Critical – 15 days
- High – 30 days
- Medium – 60 days
- Low – 90 days; and

d. Incorporate flaw remediation into the organizational configuration management process.

Discussion: The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related Controls: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI- 5, SI-7, SI-11.

Control Enhancements:

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

[Priority 1]

Control:

Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools at least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.

Discussion: Automated mechanisms can track and determine the status of known flaws for system components.

Related Controls: CA-7, SI-4.

SI-3 MALICIOUS CODE PROTECTION

[Existing] [Priority 1]

Control:

a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

   1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and

   2. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Discussion: System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the World Wide Web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious

code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, RA-5, SC-7, SC-23, SC- 28, SI-2, SI-4, SI-7, SI-8.

SI-4 SYSTEM MONITORING

[Priority 1]

Control:

a. Monitor the system to detect:
    1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:
        a. Intrusion detection and prevention
        b. Malicious code protection
        c. Vulnerability scanning
        d. Audit record monitoring
        e. Network monitoring
        f. Firewall monitoring;

        and
    2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability);
c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.

Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-17(1), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-18b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, CM-3, CM-6, CM-8, CM-11, IR-4, MA-3, MA-4, RA-5, SC-5, SC-7, SC-18, SI-3, SI-7, SR-10.

Control Enhancements:

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

[Existing] [Priority 1]

Control:

Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: None.

(4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

[Existing] [Priority 1]

Control:

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.

Discussion: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Related Controls: None.

(5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

[Existing] [Priority 1]

Control:

Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications.

Discussion: Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Related Controls: AU-4, AU-5, PE-6.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

[Existing] [Priority 2]

Control:

a. Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

Discussion: The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Related Controls: RA-5, SI-2.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

[Priority 1]

Control:

a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and

information systems that contain or process CJI; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.

Discussion: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Related Controls: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SI-3, SR-3, SR-5, SR-6, SR-10, SR-11.

Control Enhancements:

(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

[Priority 1]

Control:

Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.

Discussion: Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

Related Controls: None.

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

[Priority 1]

Control:

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.

Discussion: Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Related Controls: AU-2, AU-6, IR-4, IR-5, SI-4.

SI-8 SPAM PROTECTION

[Existing] [Priority 3]

Control:

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Discussion: System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

Related Controls: SC-5, SC-7, SI-3, SI-4.

Control Enhancements:

(2) SPAM PROTECTION | AUTOMATIC UPDATES

[Priority 3]

Control:

Automatically update spam protection mechanisms at least daily.

Discussion: Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Related Controls: None.

SI-10 INFORMATION INPUT VALIDATION

[Priority 1]

Control:

Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.

Discussion: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-

supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Related Controls: None.

SI-11 ERROR HANDLING

[Priority 3]

Control:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to organizational personnel with information security responsibilities.

Discussion: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

Related Controls: AU-2, AU-3, SI-2.

SI-12 INFORMATION MANAGEMENT AND RETENTION

[Existing] [Priority 3]

Control:

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

Discussion: Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-1, AC-6(9), AT-4,

AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-8, PS-2, PS-6, PS-7, RA-2, RA-3, RA-5, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-8.

Related Controls: AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM- 5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PS-2, PS-6, RA-2, RA-3, SA-5, SA-8, SR-2.

Control Enhancements:

(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Existing] [Priority 3]

Control:

Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

Discussion: Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

Related Controls: None.

(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

[Priority 3]

Control:

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.

Discussion: Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

Related Controls: None.

(3) INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL

[Existing] [Priority 3]

Control:

Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6.

Discussion: Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Related Controls: MP-6.

SI-16 MEMORY PROTECTION

[Priority 2]

Control:

Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization.

Discussion: Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Related Controls: SI-7.

SUPPLY CHAIN RISK MANAGEMENT (SR)

SR-1 POLICY AND PROCEDURES

[Priority 2]

Control:

a. Develop, document, and disseminate to organizational personnel with supply chain risk management responsibilities:
    1. Agency-level supply chain risk management policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;
b. Designate organizational personnel with security responsibilities to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
c. Review and update the current supply chain risk management:
    1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
    2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

Control Enhancements: None.

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

[Priority 3]

Control:

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: systems used to process, store, or transmit CJI;

b. Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Discussion: The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders.

Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation

measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

Related Controls: CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, RA-3, RA-7, SA-8, SI-4.

Control Enhancements:

(1) SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM

[Priority 3]

Control:

Establish a supply chain risk management team consisting of individuals with security responsibilities and supply chain risk management responsibilities to lead and support the following SCRM activities: information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions.

Discussion: To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

Related Controls: None.

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

[Priority 2]

Control:

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: use preferred suppliers who can provide attestation or demonstration of compliance with state or federal standards.

Discussion: The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

Related Controls: AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-10, SR-11.

SR-8 NOTIFICATION AGREEMENTS

[Priority 3]

Control:

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises to systems used to process, store, or transmit CJI.

Discussion: The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

Related Controls: IR-4, IR-6, IR-8.

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

[Priority 3]

Control:

Inspect the following systems or system components upon initial procurement and periodically as needed to detect tampering: systems used to process, store, or transmit CJI.

Discussion: The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

Related Controls: AT-3, SI-4, SI-7, SR-3, SR-5, SR-11.

SR-12 COMPONENT DISPOSAL

[Priority 3]

Control:

Dispose of CJI using the techniques and methods as described in Media Protection (MP).

Discussion: Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components.

Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information.

Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

Related Controls: MP-6.

5.20 Policy Area 20: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.20.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.20.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Identification and Authentication (IA).
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g., SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.
15. Insulate, virtually (e.g., virtual local area network (VLAN) and ACLs) or physically (e.g., firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.20.1.2 Cellular Devices

Cellular telephones, smartphones (i.e., Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.20.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a "trusted" entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.

5.20.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.20.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g., denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.

5.20.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a Wi-Fi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot's default SSID
    a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (pre-shared key)
4. Enable the hotspot's port filtering/blocking features if present
5. Only allow connections from agency-controlled devices

Note: Refer to the requirements in Systems and Communications Protection (SC) encryption for item #1. Refer to the requirements in Identification and Authentication (IA) for item #3.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.20.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
    a. Remote locking of device
    b. Remote wiping of device
    c. Setting and locking device configuration
    d. Detection of "rooted" and "jailbroken" devices
    e. Enforcement of folder or disk level encryption
    f. Application of mandatory policy settings on the device
    g. Detection of unauthorized configurations
    h. Detection of unauthorized software or applications
    i. Ability to determine the location of agency-controlled devices
    j. Prevention of unpatched devices from accessing CJI or CJI systems
    k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e., the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.20.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in System and Information Integrity (SI).

2. Are configured for local device authentication (see Section 5.20.7.1).

3. Use advanced authentication or CSO approved compensating controls as per Section 5.20.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Identification and Authentication (IA)) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.20.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third-party MDM, application, or supporting service infrastructure.

5.20.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.20.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.20.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e., laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.

3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e., tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.20.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
    a. Device known to be locked, minimal duration of loss
    b. Device lock state unknown, minimal duration of loss
    c. Device lock state unknown, extended duration of loss
    d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.20.6 Access Control

Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.20.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

5.20.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in Identification and Authentication (IA).

5.20.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Identification and Authentication (IA). If access is indirect, then AA is not required.

5.20.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.20.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.20.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.20.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e., password, PIN) to unlock the key for use

APPENDICES

This policy area contains the various appendices. The appendices are:

- Appendix A—Terms and Definitions
- Appendix B—Acronyms
- Appendix C—Network Topology Diagrams
- Appendix D—Sample Information Exchange Agreements
- Appendix E—Security Forums and Organizational Entities
- Appendix F—Sample Forms
- Appendix G—Best Practices
- Appendix H—Security Addendum
- Appendix I—References

APPENDIX A: TERMS AND DEFINITIONS

28 CFR Certification Indicator — True if the user has been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23, false otherwise. Usage information: Assertion of this privilege requires the user to have been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23. One way for a user to meet this requirement is by having taken and passed the online 28 CFR Part 23 training course and certification exam offered by the U.S. Department of Justice Bureau of Justice Assistance (BJA) via its Secured National Criminal Intelligence Resource Center (NCIRC) Web Site (http://www.ncirc.gov/securedwebsite.cfm). Alternatively, a user may meet this requirement by having taken and passed an equivalent offline 28 CFR Part 23 training course, offered by the Institute for Intergovernmental Research (IIR). (See https://28cfr.iir.com/ for details.)

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g., record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authenticator Assurance Level — The authenticator assurance level as defined by NIST SP 800-63-3. There are three defined levels: AAL1 (low), AAL2 (medium), and AAL3 (high). Usage

information: IDPs should assert this attribute to indicate the strength of the authenticator used for the current authentication process; AAL1 (low), AAL2 (medium), and AAL3 (high). AAL2 and AAL3 require multifactor authentication; although the use of multiple factors does not automatically qualify for AAL2.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient (AR) — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Authorized Recipient Security Officer (ARSO) — the individual appointed by the AR to coordinate and oversee Information Security by ensuring that the Channeler is adhering to the CJISSECPOL and Outsourcing Standard, verifying the completion of annual Security Awareness Training, and communicating with the FBI CJIS Division on matters relating to Information Security.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Basic Testing — A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing.

Comprehensive Testing — A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate — Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately

completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client — A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing — A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider — An organization that provides cloud computing services.

Cloud Subscriber — A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy**.**

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Controlled Unclassified Information (CUI) — Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. (32 CFR Vol 6 Part 2002)

Counter Terrorism Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for counter-terrorism data and documents within the user's home system, network, or agency. False otherwise. Usage information: Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal history data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include National Crime Information Center (NCIC) Criminal History. User eligibility requirements are decided by federation members, but may include: Fingerprint (FP) based background, NCIC training, access to Law Enforcement criminal history data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Criminal History Record Information (CHRI) — Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions,

indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

Criminal Intelligence Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal intelligence data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Criminal Law Enforcement Reporting Information System (CLERIS), Regional Information Sharing Systems (RISS), Joint Regional Information Exchange System (JRIES), and Law Enforcement Intelligence Units (LEIU). User eligibility requirements are decided by federation members, but may include: 28 CFR (23) training, Fingerprint (FP) based background, access to intelligence data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Criminal Investigative Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal investigative data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Criminal Law Enforcement Reporting Information System (CLERIS) and Contact and Information Management System (CIMS). User eligibility requirements are decided by federation members, but may include: Fingerprint (FP) based background, access to investigative data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Data Center — A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.

Decryption — The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g., solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media — Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature — A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Display Name — The user's display name is a text string formatted for display purposes in applications and correspondence.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Email Address Text — The electronic mailing address by which the user may be contacted.

Employer Name — The name of the organization that is the user's primary employer.

Employer ORI — A unique identifier assigned to the organization that is the user's primary employer. ORIs are generally assigned by the FBI; however, in some cases they may be assigned by other agencies.

Employer Organization General Category Code —The general category of the organization that is the user's primary employer.

Employer State Code — The state, commonwealth, province, or other such geopolitical subdivision of the country in which is located the primary business office of the organization that is the user's primary employer.

Encryption — A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort — Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) — Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federation Assurance Level — There are 3 Federation Assurance Levels representing the assurance level of the user's federated assertion: FAL1 (low assurance), FAL2 (moderate assurance), and FAL3 (high assurance) based on NIST SP 800-63-3. Usage information: IDPs

should assert this for all assertions sent to RPs correctly identifying the level of assurance of the assertion. The RP can also derive the FAL if not asserted.

Federation Id — The persistent, federation-unique identifier for the user, comprising a federation part, an optional trusted identity broker (TIB) part, an identity provider (IDP) part, and a local ID.

Focused Testing — A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g., Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g., malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

General User — A user, but not a process, who is authorized to use an information system.

Given Name — The first name of the user.

Government Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for government data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Tax Data, Labor Data, Uniform Commercial Code (UCC) Filings, Property Records, Department of Motor Vehicles (DMV), Drivers License (DL), Boat Ownership, Corporate Records, and Protected Critical Infrastructure Information (PCII). User eligibility requirements are decided by federation members, but may include: Agency vetting, application training, state law, and Federal law. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e., hash value) to be used as a representative of that data.

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution, the asymmetric encryption keys are used for client/server certificate exchange to provide session

integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity Assurance Level — The maximum NIST identity assurance level as defined by NIST SP 800-63-3 for which the identity proofing process of this Identity Provider Organization qualifies. There are three defined levels: IAL1 (low), IAL2 (medium), and IAL3 (high). Usage information: IDPs should use this attribute to indicate the assurance level of their identity and attribute proofing processes.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Identity Provider Id — The unique identifier within the federation that identifies the identity provider (IDP) of the user within the federation. Comprises a federation part, an optional trusted identity broker (TIB) part, and an identity provider (IDP) part. The general format of an identity provider ID is: "{Federation}:[TIB:{TIB}:]IDP:{IDP}". Usage information: This identifier MUST be consistent with the federation identifier, IDP identifier, and (if applicable) TIB identifier denoted within the user's Federation Id attribute.

In-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access — Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g., CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law

enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Intelligence Analyst Indicator — True if the user is an Intelligence Analyst (IA) for a government agency, false otherwise. Usage information: An Identity Provider (IdP) may assert that a user is an IA if they work for a government agency, and/or company who works with the government, in order to provide information assessments about criminal or security threats.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A criminal justice agency (including law enforcement) or any federally authorized agency/entity, other than a CSA or State Identification Bureau (SIB), that leverages a direct connection to the FBI CJIS Division.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as "root access") of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices — Laptop devices are mobile devices with a full-featured operating system (e.g., Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g., smartphones), or mobile devices that feature a limited-feature operating system (e.g., tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g., Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). There operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Local Id — The unique local identifier associated with the user for internal purposes within the user's identity provider (IDP). This identifier is assigned and maintained by a federation member agency or partner organization and used for local authentication and identification. The identifier typically has local significance and is integrated into the existing legacy IT infrastructure and/or business processes of the federation member agency or partner organization.

Logical Access — The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning — When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g., cellular, Wi-Fi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets.

Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (Wi-Fi) Hotspot — A mobile (Wi-Fi) hotspot is a zone or area associated with a mobile device (e.g., smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

NCIC Certification Indicator — True if the user has a valid, active certification in the usage and handling of data in accordance with National Crime Information Center (NCIC) rules and regulations, false otherwise.

N-DEx Privilege Indicator — True if the user has privileges to access the Federal Bureau of Investigation (FBI) Law Enforcement National Data Exchange (N-DEx), false otherwise. Usage information: Assertion of this privilege requires the user to meet certain requirements which are not currently documented in the GFIPM Metadata Specification. Future versions of this spec will properly document these requirements. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Non-digital Media — Non-digital media means a hard copy or physical representation of information, including, but not limited to, paper copies, printer ribbons, drums, microfilm, platens, and other forms of preserved or preservable information.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Organizational Personnel with Security Responsibilities — Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning — Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) — An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

PCII Certification Indicator — True if the user has a valid, active certification in the usage and handling of Protected Critical Infrastructure Information (PCII) data in accordance with US Department of Homeland Security (DHS) rules and regulations, false otherwise. Usage information: Information about PCII authorized user training is available at the following URL. http://www.dhs.gov/receive-pcii-authorized-user-training

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access — The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g., the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media — Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning — When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device — Pocket/Handheld mobile devices (e.g., smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Privileged User — A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.

Property Data — Information about vehicles and property associated with a crime.

Public Safety Officer Indicator — True if the user is a public safety officer (PSO), false otherwise. Usage information: An IDP may assert that a user is a PSO if the user is authorized to act in a role pursuant to the safety and welfare of the public within a government jurisdiction. This may include firefighters, emergency medical technicians (EMTs), hazardous materials (HAZMAT) cleanup specialists, etc.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) — A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as "root access") of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting — The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g., SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) — Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone — See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency — A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Sur Name — The last name or family name of the user.

Sworn Law Enforcement Officer Indicator — True if the user is a sworn law enforcement officer (SLEO), false otherwise. Usage information: An IDP may assert that a user is a SLEO if all of the following conditions are true.

1. The user is a full-time employee of a state-recognized law enforcement agency.
2. The user is authorized (has the authority) to make an arrest.
3. The user is certified by a State Certifying Authority (i.e., Peace Officer Standards and Training (POST)), or equivalent.

Alternatively, an IDP may assert that a user is a SLEO if the user is a full time employee of a state-recognized law enforcement agency, acting on behalf of a SLEO, in performance of the user's assigned duties. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices — Tablet devices are mobile devices with a limited-feature operating system (e.g., iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g., smartphones) or mobile devices with full-featured operating systems (e.g., laptops).

Telephone Number — The telephone number for a telecommunication device by which the user may be contacted.

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

Unique Subject Id — A persistent unique identifier for the subject or user that identifies both the subject or user and their identity provider. The identity provider should be identified by a fully qualified domain name.

User Certificate (user-based) — Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort — Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) — See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point — A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (Wi-Fi) Hotspot — A wireless (Wi-Fi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B: ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CISA	Cybersecurity & Infrastructure Security Agency
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
CUI	Controlled Unclassified Information

DAA	Designated Approving Authority
DoJ	Department of Justice
DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control

MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing & Analysis Center
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance

QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TSC	Threat Screening Center
TLS	Transport Layer Security
UCN	Universal Control Number
USCERT	U.S. Computer Emergency Readiness Team
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C: NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e., topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJI, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency's documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific "moving parts" in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency's network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the "major moving parts" for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

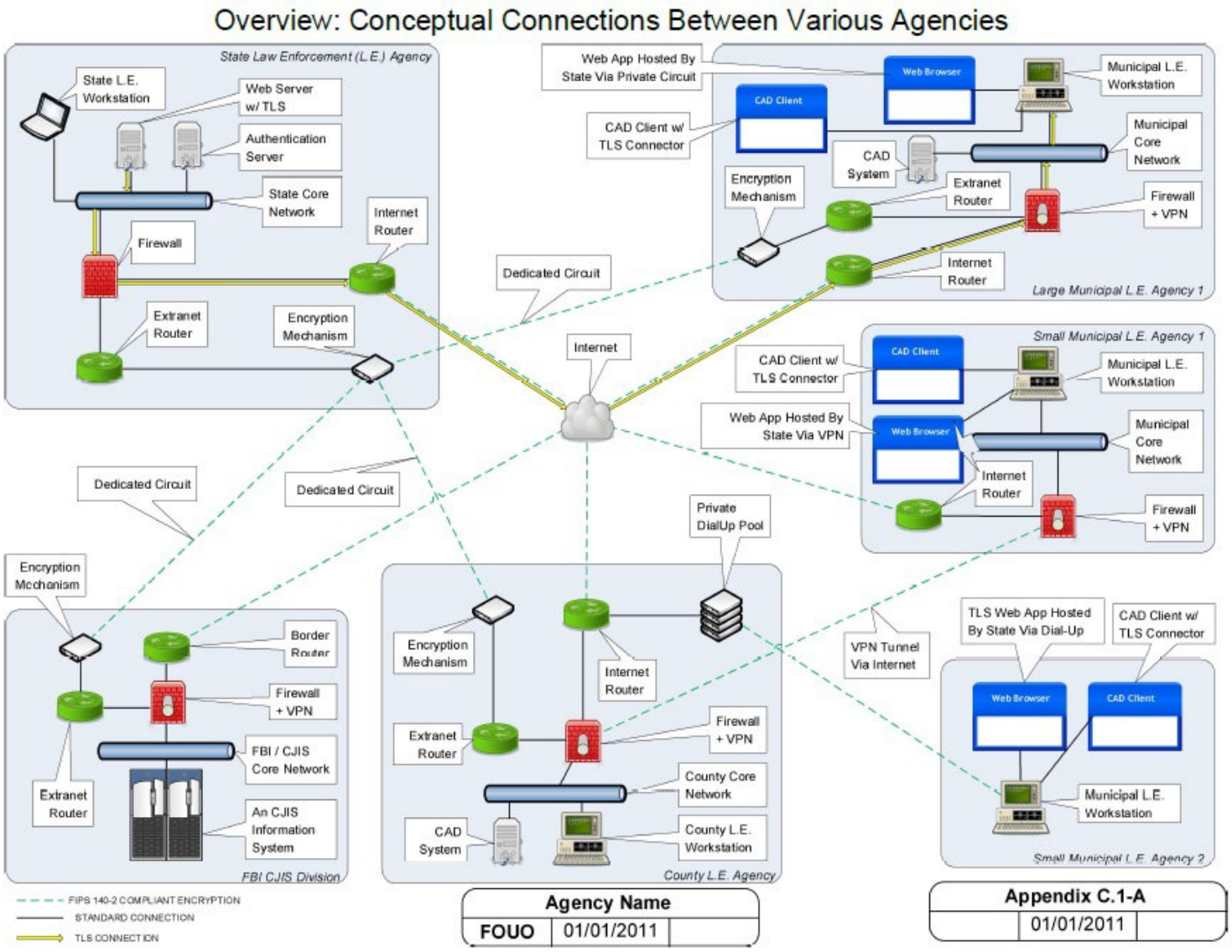


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

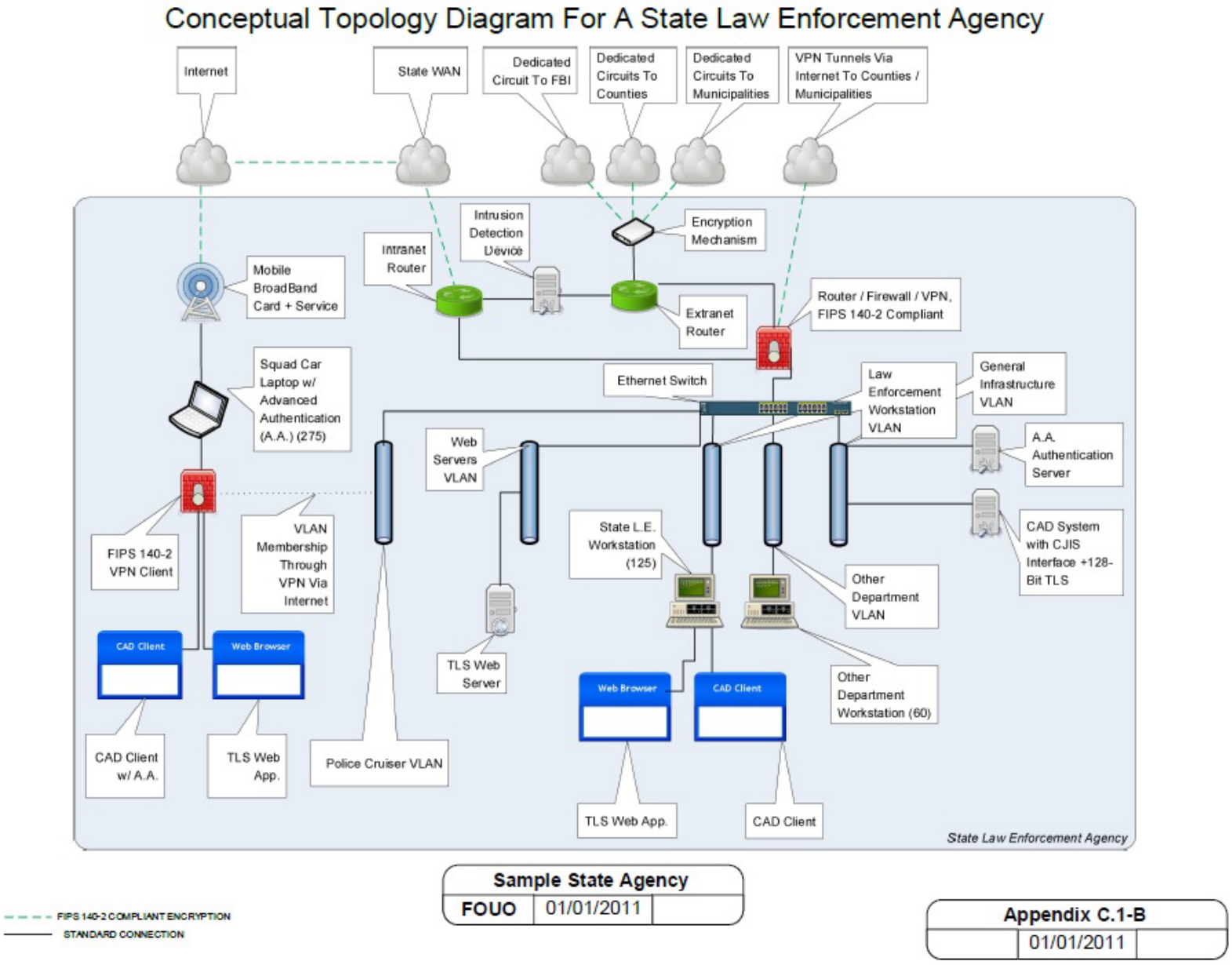


Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

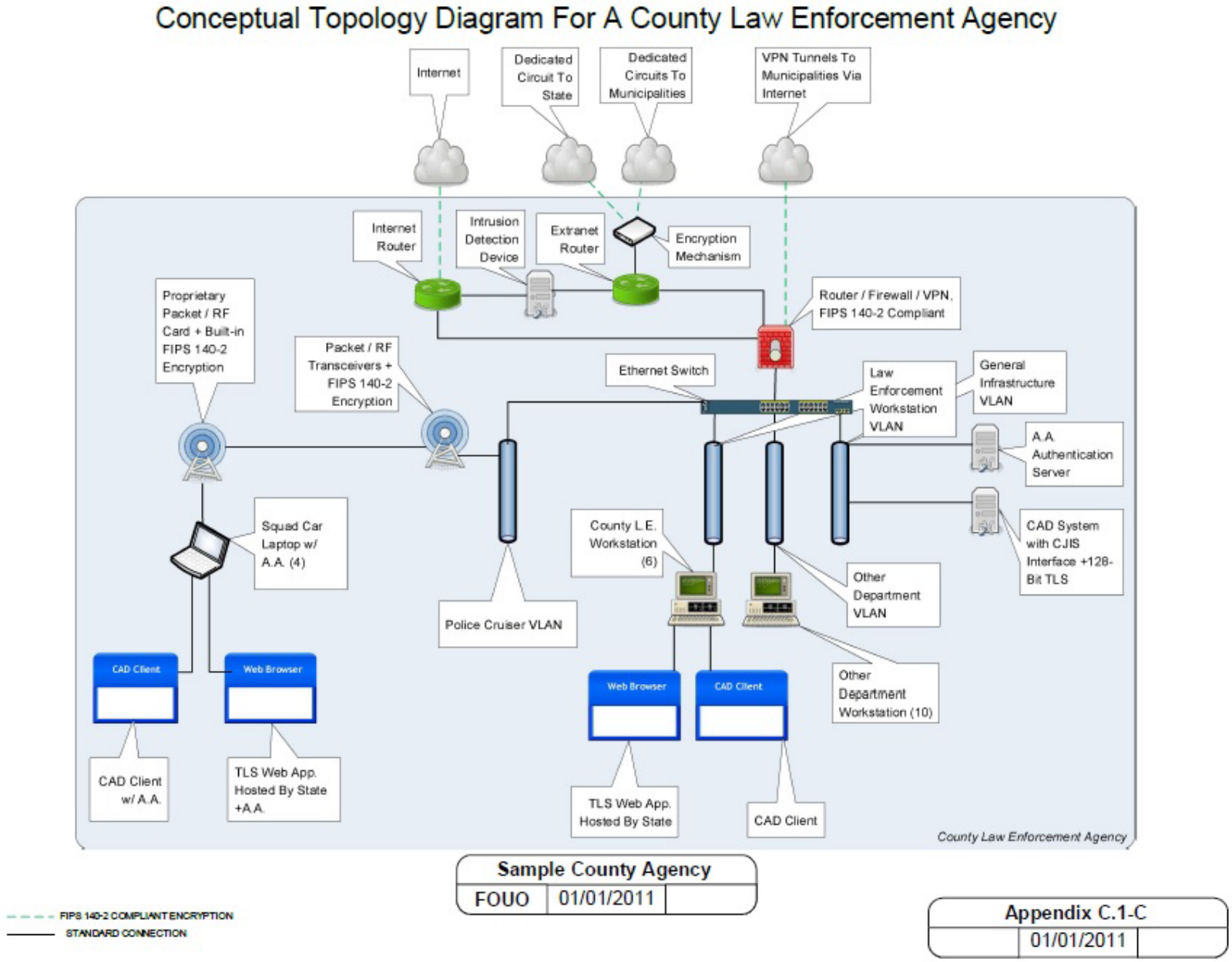
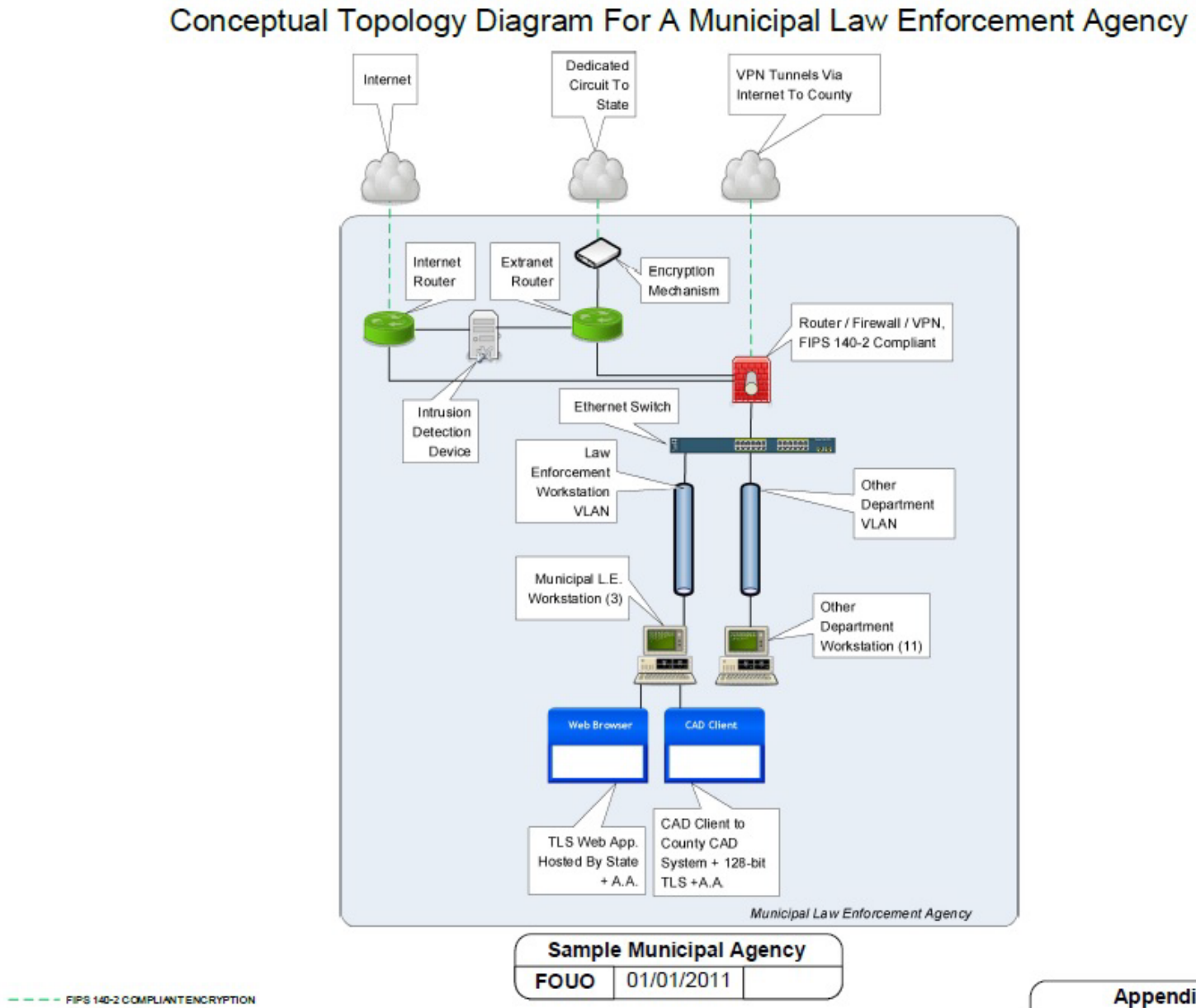


Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency



APPENDIX D: SAMPLE INFORMATION EXCHANGE AGREEMENTS

This appendix contains sample information exchange agreements.

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) DIVISION'S SYSTEM AND PROGRAM USER AGREEMENT

The FBI's CJIS Division provides state-of-the-art systems, programs, and services to the federal, state, local, tribal, regional, territorial, and foreign criminal and noncriminal justice communities. Through a shared management concept, the CJIS Division's systems, programs, and services are administered and maintained by the FBI's CJIS Division and managed in cooperation with the CJIS Advisory Policy Board (APB) and the Council established by the National Crime Prevention and Privacy Compact Act of 1998 (Compact). The CJIS Division's System and Program User Agreement (hereafter referenced as the User Agreement) covers the following: Law Enforcement Enterprise Portal (LEEP); National Crime Information Center (NCIC); National Instant Criminal Background Check System (NICS); National Data Exchange (N-DEx) System; Next Generation Identification (NGI) System; and the Uniform Crime Reporting (UCR) Program.

This User Agreement is intended to identify the categories of users, as defined by the *CJIS Security Policy (CJISSECPOL)*, and outlines the roles and responsibilities associated with participating in the CJIS Division's systems, programs, and services available to the above-listed criminal and noncriminal justice communities. This User Agreement identifies additional documentation as a valuable resource available to those individuals responsible for reviewing and signing the User Agreement.

PART 1-USER DEFINITIONS

A **CJIS Systems Agency (CSA)** is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the criminal justice information (CJI) from various systems managed by the FBI's CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to FBI CJIS Division's systems.

A **CJIS Systems Officer (CSO)** is an individual located within the CSA responsible for the administration of the CJIS network for the CSA.

An **Interface Agency (IA)** is a criminal justice agency (including law enforcement) or any federally authorized agency/entity, other than a CSA or State Identification Bureau (SIB), that leverages a direct connection to the FBI CJIS Division.

An **IA official** is an employee of the IA responsible for planning necessary hardware, software, funding, and training for the IA's authorized access to the CJIS Division's systems. The IA official shall not be a contract employee.

A **SIB** is the state (to include United States (U.S.) territories) agency with the responsibility for the state's fingerprint identification services.

An **SIB Chief** is the designated manager of the state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

A **state Compact officer** is the representative of a state that is party to the Compact and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

The **FBI Compact officer** is appointed by the Director of the FBI and is responsible for administering the Compact within the Department of Justice and other federal agencies.

PART 2-CJIS DIVISION'S SYSTEMS, SERVICES, PROGRAMS AND RESPONSIBILITIES

The FBI's CJIS Division makes available access to the following systems and major programs (Note: Place a checkmark in the bulleted box to indicate use of specific service(s) by the agency reviewing and signing this User Agreement (applicable documents identified in Part 3):

- ❑ LEEP
- ❑ NCIC
- ❑ NICS
- ❑ N-DEx
- ❑ NGI
- ❑ UCR

The FBI CJIS Division supports a multitude of services within the above-listed systems and programs (e.g., Interstate Identification Index (III) within NGI, NCIC offline search, UCR's Law Enforcement Suicide Data Collection, and LEEP's virtual command centers).

The FBI's CJIS Division provides the following to its authorized users, as applicable:

1. Operational, technical, and investigative assistance.

2. Secure telecommunication methods, such as wide area network (WAN) and virtual private network (VPN) connections.

3. Timely information on the CJIS Division's systems, programs, and services, by means of procedures and operating manuals, policy and implementation guides, code manuals, technical and operational updates, web pages, presentations, brochures, various newsletters, CJIS Information Letters, frequently asked questions, and other relevant documents.

4. On-site and virtual training, assistance, and system and program reference materials. The FBI's CJIS Division may prioritize on-site training opportunities to CSAs, SIBs, or IAs with open compliance findings, FBI priority initiatives, or other time-sensitive matters impacting the criminal and noncriminal justice communities.

5. Ongoing assistance through meetings and briefings to discuss operational and policy issues.

6. The CJIS Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS systems, programs, and services.

7. The Compact Office through education and assistance concerning the noncriminal justice use of the III of the NGI System, including facilitating engagement with the Compact Council, as needed.

8. Formal audits to ensure compliance with applicable statutes, regulations, and policies.

PART 3-CJIS DIVISION'S SYSTEMS AND PROGRAM DOCUMENTS AND AUTHORITIES

The following documents and authorities are incorporated by reference and made part of this User Agreement regarding agency access and use; this list is not all inclusive. Other policies, regulations, and manuals will be developed, published, and/or amended as CJIS Division systems, programs, and services evolve. Please contact the appropriate program office and visit the FBI CJIS Division's website for additional information: www.fbi.gov/cjis.

Security and Information Exchange Documents

CJISSECPOL

The CJISSECPOL provides criminal justice and noncriminal justice agencies with the minimum set of security requirements for access to FBI CJIS Division systems and information and to protect and safeguard CJI.

Information Exchange Package Documentation (IEPD)

An IEPD is a specification for a data exchange and defines a particular data exchange for a system.

Enterprise Documents

CJIS Information Letters

These letters provide users of CJIS Division's systems and programs with policy and procedural updates.

CSO Reference Guide

The purpose of this guide is to provide an overview of the roles and responsibilities of the CSO position.

LEEP Documents

LEEP Procedures and Operations Manual

This manual addresses the roles, responsibilities, and commitments between Identity Providers, Service Providers, and the FBI.

NCIC Documents

NCIC Operating Manual

This manual provides guidelines on the proper operation and use of the NCIC System, including the standards, procedures, formats, rules, and criteria.

NCIC Technical and Operational Updates (TOUs)

TOUs are documents that describe technical and operational changes to the NCIC System.

NICS Documents

NICS Policy Reference Guide

This manual serves as a training guide for NICS Point-of-Contact states who are processing name-based background checks through NICS before transferring a firearm to a prospective transferee.

Disposition of Firearms (DoF) User Guide

This manual serves as a training guide for law enforcement and criminal justice agencies disposing of (returning) firearms.

NICS Resource Entry and Maintaining Entries into the NICS Indices User Guide

This manual serves as a guide to sufficient source documentation to support a NICS Indices entry upon appeal or audit.

NICS Indices Reference Guide for Contributors

This manual serves as a guide for entering information into the NICS Indices.

N-DEx Documents

N-DEx Policy and Operating Manual

This manual applies to all entities with access to, or who operate in support of, N-DEx System, services, and information.

NGI Documents

III/National Fingerprint File (NFF) Operational and Technical Manual

This manual describes the III and NFF programs, including technical and operational details; procedures for entering, maintaining, and updating III and NFF records; and requirements for criminal and noncriminal fingerprint submissions.

III TOUs

TOUs are documents that describe technical and operational changes to the III System.

Electronic Biometric Transmission Specification (EBTS)

The purpose of the EBTS is to provide standards for electronically encoding and transmitting biometric images, identification, and arrest data which extends the American National Standards Institute/National Institute of Standards and Technology and Information Technology Laboratory standard. These standards ensure data is formatted for acceptance into NGI.

Compact Council's Security and Management Control Outsourcing Standards

These documents provide noncriminal justice agencies with information on the required procedures, responsibilities, and controls to maintain adequate security and integrity of criminal history record information (CHRI) while under the control or management of an outsourced, third-party contractor.

NGI Interstate Photo System (IPS) Policy and Reference Guide

This guide is made available to authorized law enforcement users and describes the policy and technical requirements for authorized use of the NGI IPS, as well as the best practices for NGI IPS users. It describes the types of NGI IPS enrollment and search transactions accepted, responses returned, training required, and additional resources available for NGI IPS users.

NGI Rap Back Service Criminal Justice Policy and Implementation Guide

This guide informs the SIBs and federal agencies of the policy and technical requirements for participation in the criminal justice Rap Back Service.

NGI Rap Back Service Noncriminal Justice Policy and Implementation Guide

This guide provides policy, technical, legal, and privacy requirements to the SIBs, federal submitting agencies, and authorized contractors who choose to participate in the FBI's NGI Noncriminal Justice Rap Back Service.

NGI Rap Back Service Noncriminal Justice Outsourcing Policy and Implementation Guide

This guide provides direction on the required policies and operations for FBI-approved channelers and nonchannelers who assist an authorized recipient with their noncriminal justice participation in the FBI's NGI Rap Back Service.

NGI Repository for Individuals of Special Concern (RISC) Policy and Implementation Guide

This guide is for the use of CSAs, vendors, and authorized criminal law enforcement agency interested in the mobile fingerprint identification search of the NGI RISC. It defines the types of search transactions that are accepted, the types of responses returned to contributors, and the system description.

NGI Iris Service Policy and Implementation Guide

This guide includes the policy and technical requirements for authorized criminal justice agency users to utilize the NGI Iris Service. It defines the types of NGI Iris Service enrollments and search transactions that are accepted, the responses returned, and references to additional technical resources.

UCR Documents

NIBRS User Manual

This manual is used to assist law enforcement agencies in reporting their crime statistics via NIBRS. This manual addresses NIBRS policies, including but not limited to, the types of offenses reported via NIBRS and guidelines for an agency to become certified to submit NIBRS data to the FBI.

NIBRS Technical Specification

This manual provides information necessary to create proper UCR NIBRS flat file submissions and is to be used in conjunction with the *NIBRS User Manual*.

Hate Crime Data Collection Guidelines and Training Manual

This manual is intended to assist law enforcement agencies in establishing an updated hate crime training program to allow their personnel to collect and submit hate crime data to the FBI's UCR Program.

Cargo Theft User Manual

This manual identifies policy and provides information regarding the types of offenses that constitute a cargo theft incident, how to identify a cargo theft, and guidelines for reporting cargo theft.

National Use-of-Force Data Collection Flat File and Bulk Load Technical Specification

This manual provides the record layout for report segments and related data elements. The bulk load feature enables report submissions outside of the web application interface.

Authorities

Title 28, United States Code (U.S.C.), Section 534

Among other things, 28 U.S.C.§ 534 authorizes the United States Attorney General to collect, preserve, and exchange identification, criminal identification, crime, and other records.

Title 28, Code of Federal Regulations (C.F.R.), Part 20 and the Appendix

The purpose of these regulations is to ensure that CHRI, wherever it appears, is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy. These regulations apply to authorized federal, state, local, tribal, foreign, and international criminal justice agencies to the extent that they access the various criminal justice information systems managed by the CJIS Division or use or disseminate the records and information residing in those systems.

28 C.F.R., Part 25

The purpose of this subpart is to establish policy and procedures implementing the Brady Handgun Violence Prevention Act.

28 C.F.R. § 50.12

This section is intended to ensure that all relevant criminal record information is made available to provide for the public safety and further to protect the interest of the prospective employee/licensee who may be affected by the information or lack of information in an identification record.

Title 34, U.S.C. § 40311-40316

The Compact Act provides the legal framework for the noncriminal justice use of the III system and to facilitate complete decentralization of criminal history records. Established pursuant to the Compact, the Compact Council is to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

PART 4- RESPONSIBILITIES OF THE CSA/IA/SIB

The purpose of a designated CSA/IA/SIB (also referenced as Signatory) is to unify responsibility for the administration and oversight of the users of the CJIS Division's systems, programs, and services, and ensure adherence to established procedures and policies within each Signatory federal, state, local, tribal, regional, territorial, and foreign agency and by each user. The CSA/IA/SIB may impose more stringent protection measures than outlined in this User Agreement. Such decisions shall be documented and kept current.

In addition, and as applicable, the CSO/IA official acknowledges state and FBI Compact officer responsibilities to ensure that Compact statutory provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective area of responsibility.

Furthermore, this User Agreement applies to SIBs who have access to the CJIS Division's systems separate and apart from their state's CSA. In addition, and as applicable, the SIB Chief acknowledges the state Compact officers' responsibilities to ensure that Compact statutory provisions and rules, procedures, and standards are complied with in their respective area of responsibility.

To ensure continued access as set forth above, the Signatory agrees to adhere to all applicable policies of the CJIS Division including, but not limited to, the following:

1. As applicable, the Signatory agencies will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, federal, state, local, tribal, regional, territorial, and foreign agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by federal, state, local, tribal, regional, territorial, and foreign laws, and, where applicable, continue to move toward participation in the III and, upon ratification of the Compact, the NFF. [Article I(4) of the National Crime Prevention and Privacy Compact Act (Title 34, United States Code, section 40316) defines criminal history records as (A) . . . information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; and (B) does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.]

2. Appropriate and reasonable quality assurance procedures, e.g., hit confirmation, audits for record timeliness, and validation for all CJIS Division systems, programs, and services in which they participate, e.g., biometrics, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Division's systems.

3. Biannual file synchronization of information entered into the III by participating agencies.

4. Each Signatory is responsible for the minimum-security measures as defined by the *CJISSECPOL*.

5. Each CSA/IA/SIB is responsible for completing a triennial audit of all agencies with access to the CJIS Division's systems through the system(s) of the CSA/IA/SIB. In addition, each authorized CSA/IA/SIB user is subject to a triennial audit by the CJIS Division.

6. Each CSA/IA/SIB shall be responsible for training requirements, including compliance with operator training mandates of the CJIS Division's systems, programs, and services, as outlined by the above-referenced systems and program documents.

7. Each CSA/IA/SIB shall be responsible for maintaining the integrity of their information systems in accordance with established policies to ensure only authorized terminal access; only authorized transaction submission; and proper protection, handling, and dissemination of CJI. Each CSA/IA/SIB shall be responsible for security incident reporting as required by the *CJISSECPOL*.

8. In the event that any state/local/tribal agency for which the designated CSA/IA/SIB is responsible receives a request pursuant to a freedom of information law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose FBI information concerning the subject matter of this agreement, the designated CSA/IA/SIB will ensure that the state/local/tribal agency immediately notifies the FBI of any such request in order to allow the FBI sufficient time to seek to protect its equities through appropriate channels, if necessary. For purposes of this paragraph, FBI information includes, but is not limited to, e-mails or other correspondence with the FBI and the information referenced in Part 2, paragraphs 3 through 5 of this agreement. This provision survives the termination of this agreement.

PART 5-GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each signatory to this User Agreement (hereafter referenced as party) shall bear its own costs in relation to this User Agreement. Expenditures will be subject to budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this User Agreement in no way implies that Congress will appropriate funds for such expenditures.

Termination and Other Topics

1. All activities of the parties under this User Agreement will be carried out in accordance with the above-described provisions.

2. This User Agreement may be amended or terminated by the mutual written consent of the parties' authorized representatives.

3. The parties acknowledge that this User Agreement does not alter applicable law governing any claim for civil liability arising out of any activity conducted pursuant to this User Agreement or otherwise relating to this User Agreement.

4. This User Agreement is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, the United States, or the officers, employees, agents, or other associated personnel thereof. No assignment of rights, duties, or obligations of this User Agreement shall be made by any party without the express written approval of a duly authorized representative of all other parties.

5. Each party agrees to notify the other party in the event of receipt of a civil claim arising from this User Agreement. The parties agree to cooperate fully with one another in the event of any investigation arising from alleged negligence or misconduct arising

from acts or omissions related to this User Agreement. Nothing in this paragraph prevents any party from conducting an independent administrative review of any incident giving rise to a claim.

6. Either party may terminate this User Agreement upon 30-days, written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

a. The parties will continue participation, financial or otherwise, up to the effective date of termination.

b. Each party will pay the costs it incurs as a result of termination.

c. All information and rights therein received under the provisions of this User Agreement, prior to the termination, will be retained by the parties subject to the provisions of this User Agreement.

PART 6-ACKNOWLEDGMENT AND CERTIFICATION

I hereby certify that I am a U.S. Citizen and acknowledge the duties and responsibilities as set out in this User Agreement. I acknowledge these duties and responsibilities have been developed and approved by the users of the CJIS Division's systems to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Division's systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of non-monetary sanctions against the offending signatory agency. The APB or the Compact Council may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this User Agreement and all applicable federal and state laws and regulations relevant to the receipt and dissemination of information provided through the CJIS Division's systems, programs, and services.

Should the designated official vacate their position, the FBI designated federal officer must be notified via E-mail at AGMU@leo.gov. The name and telephone number of the acting CSO, IA official, or SIB chief and when known, the name and telephone number of the new CSO, IA official, or SIB chief must be provided, and a new User Agreement must be executed by the appropriate designated official. In addition, if the use and participation in the acknowledged systems and/or programs in Part 2 of this User Agreement change, a new User Agreement must be executed. In addition, this User Agreement will be reviewed every three years by the FBI CJIS Division.

This User Agreement is a formal expression of the purpose and intent of the parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of the parties. The "Acknowledgment and Certification" is being executed by the appropriate authorized official in a representative capacity. Accordingly, this User Agreement will remain in effect after the authorized official vacates his/her position or until it is affirmatively amended or rescinded in writing. This User Agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

PART 7-SIGNATORY AUTHORITY

You are signing this CJIS Division's System and Program User Agreement as one of the following officials: CSO, IA Official, or SIB Chief.

CSO and CSA SIGNATORIES

_____ Date: _____
CJIS Systems Officer
(Name)
(Title)
(Agency Name)

CONCURRENCE OF CSA HEAD:

_____ Date: _____
CSA Head

INTERFACE AGENCY SIGNATORY

_____ Date: _____
Interface Agency Official
(Name)
(Title)
(Agency Name)

CONCURRENCE OF INTERFACE AGENCY HEAD:

_____ Date: _____
Interface Agency Head

STATE IDENTIFICATION BUREAU SIGNATORY

_____ Date: _____
State Identification Bureau Chief
(Name)
(Title)
(Agency Name)

CONCURRENCE OF STATE IDENTIFICATION BUREAU AGENCY HEAD:

_____ Date: _____
State Identification Bureau Agency Head

FBI CJIS DIVISION SIGNATORY

_____ Date: _____
Name of Assistant Director
Assistant Director
FBI CJIS Division

Revised: 08/25/2023

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

(1) Priorities.
(2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
(3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
(4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
(5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

"…management control of the criminal justice function remains solely with the Criminal Justice Agency." Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

_____ _____
John Smith, CIO Date
Any State Department of Administration

_____ _____
Joan Brown, CIO Date
(Criminal Justice Agency)

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. BACKGROUND: The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. AUTHORITY: The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. SCOPE:

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.
ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.
iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.
iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.
v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.
vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.
vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.
viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.
ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco

Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.
ii. Purchase hardware and software that are compatible with the CJIS WAN.
iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.
iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.
v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.
vi. Pay for all telecommunication requirements related to its connectivity.
vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.
viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.
ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.
x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).
xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.
xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).
xiii. Transport only official, authorized traffic over the Secure VPN.
xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above – described provisions.
b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.
c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.
ii. Each party will pay the costs it incurs as a result of the termination.
iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

_____ _____

[Name] Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

_____ _____

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
Wide Area Network (WAN) USER AGREEMENT
BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;

- Training assistance and up-to-date materials provided to each designated agency official, and;

- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;

- *Title 28, Code of Federal Regulations, Part 20*;

- Computer Incident Response Capability (CIRC);

- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.

2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.

3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.

4. Security – Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit – Each agency shall be responsible for complying with the appropriate audit requirements.

6. Training – Each agency shall be responsible for training requirements, including compliance with training mandates.

7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent

connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability;* and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*_____ _____

Signature Print or Type

CJIS WAN Agency Official Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*_____ _____

Signature Print or Type

*_____ _____

Title Date

State CSO

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director _____

Title Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E: SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC)
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F: SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

_____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

_____

SYSTEM(S) AFFECTED: _____

_____

SYSTEM(S) AFFECTED (e.g., CAD, RMS, file server, etc.): _____

_____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

_____

_____

Copies To:

John C. Weatherly
(FBI CJIS Division ISO)
1000 Custer Hollow Road
Clarksburg, WV 26306-0102
(304) 625-3660
iso@fbi.gov

APPENDIX G: BEST PRACTICES

This appendix contains best practices.

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008 http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx:

> *"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."*

From a trade publication, kernelthread.com http://www.kernelthread.com/publications/virtualization/:

> *"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."*

From an Open Source Software developer http://www.kallasoft.com/pc-hardware-virtualization-basics/:

> *"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:*
>
> - *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
> - *"Type-2 Hypervisor which requires a separate application to run within an operating system*
>
> *"Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For*

instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system."

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

"Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Sever 2008 Hyper-V, and is fully support by both companies' channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments."

"Sun Microsystems today account the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for SunxVM Server software and contribute to the direction and development of the product."

"NetEx, specialist in high-speed data transport over TCP, today announced Vistual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide –area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company's award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network."

From several sources, particularly:

http://www.windowsecurity.com/articles/security-virutalization.html
http://csrc.nist.gov/publications/drafts/6--=64rev2/draft-sp800-64-Revision2.pdf

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.

- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply "least privilege" technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e., Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) – A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.

b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the

company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.

b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic "CIA"). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and

denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain

confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as

a result of malicious actions. Misuse may involve legitimate users (i.e., insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion – An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state – At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g., “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

9. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.

- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.

- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).

- Use Ipsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for Ipsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal

Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

10. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

11. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

12. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are

communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

13. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g., susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

14. If practical, "softphone" systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of "softphones", for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

15. If mobile units are to be integrated with the VoIP system, use products implementing Wi-Fi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent Wi-Fi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (Ipsec) with FIPS 140-2 validated

cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

16. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The "cloud" spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, "Can an Agency be compliant with the CJIS Security Policy and also cloud compute?"

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren't new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)

- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)

- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)

- Are the encryption requirements being met? (5.10.1.2 Encryption)
    - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
    - Is the data encrypted while at rest and in transit?

- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
    - Will the cloud subscriber be notified of any incident?
    - If CJI is compromised, what are the notification and response procedures?

- Is the cloud service provider a private contractor/vendor?
    - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)

- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
    - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
    - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

   Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

   Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

   Note: When selecting a cloud service provider, the CJIS ISO Program reminds agencies the CJIS Security Policy sets the minimum requirements for the protection of CJI. Additional security assurances from other authorizations such as FedRAMP, StateRAMP, SOC Type 2, etc., may be leveraged, however, they do not guarantee compliance with the CJIS Security Policy.

   a. <u>Scenario 1–Agency Stores CJI in a Cloud:</u>
      A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption

keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

b. Scenario 2–Agency Accesses CJI While in a Cloud:
A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump* Recovery:
A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

* Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

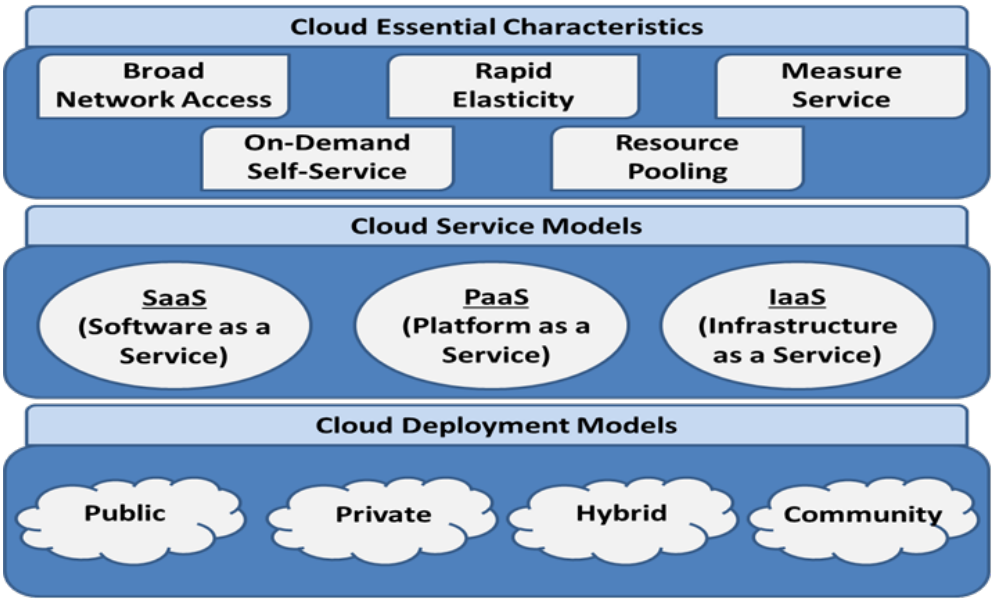


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

* *Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Cloud providers offer different levels of service, i.e.; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The way CJI is placed and accessed in the cloud determines if the personnel security requirements in Section 5.12 apply. Access to encryption keys and management of the resources vary depending on what type of service is used. The SaaS offering is the most likely service wherein the cloud service provider may have access to unencrypted CJI due to software updates, patches, and management. However, through management and control of encryption keys, all service offerings may be implemented in an agency-controlled manner where the cloud service provider has no ability to access unencrypted CJI.

For cloud computing services that involve the storage, processing, or transmission of CJI, Section 5.12 security terms and requirements apply to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI. It is critical for the agency to understand the level of service and access required for each cloud implementation.

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

> ** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

> ** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

<u>Governance</u>

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory

compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over

privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such

information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools

resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g., encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.

- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.

- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and

preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.

Areas	Recommendations
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. • Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolvement of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g., Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g., Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g., cellular service, Wi-Fi + Cellular, Wi-Fi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a Wi-Fi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the

device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full-featured operating system (e.g., Windows or a Linux variant). Also included in this category are 'tablet' type full-featured computers running a traditional full-featured operating system but without an attached keyboard. The main defining factor is the use of a full-featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via Wi-Fi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g., network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g., cellular or Wi-Fi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g., auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g., Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited-feature operating system (e.g., Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited-feature sets. Additionally, limited functionality

operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can function effectively on the devices (e.g., traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g., 'always on cellular' vs. Wi-Fi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or 'holster' attached to the body. The bulk of this category will be cellular 'smartphones' with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g., portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full-feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g., device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), Wi-Fi Only (includes 'on demand' cellular), and Cellular (always on) + Wi-Fi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either

through the operating system or a third-party mobile device management (MDM) system may be able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by 'always on' network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with 'always on' cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as 'always on' or 'on demand'. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain 'airplane' mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g., standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other 'eavesdropping' devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g., web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a 'personal firewall' if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full-featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an 'always on' cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

Wi-Fi only (includes 'on-demand' cellular)

Wi-Fi only devices do not include cellular radios or include cellular radio that must be manually activated or 'connected' to the cellular network. They connect to the network or internet through Wi-Fi 'hotspots' or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific Wi-Fi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any Wi-Fi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted Wi-Fi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over 'public' Wi-Fi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g., MDM based policy) that only allow devices to connect to cryptographically verified agency controlled Wi-Fi access points.

Wi-Fi only or devices with 'on-demand' cellular access (e.g., user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking ('bricking') or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full-featured laptops but may not be available for limited-feature mobile operating systems.

Cellular (always on) + Wi-Fi Network

This is a hybrid scenario that has become typical with most 'smartphones'. These devices contain both the always on cellular connection, but may also be configured to access local Wi-Fi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the Wi-Fi scenario unless the capability of the device to connect to Wi-Fi networks is limited by technology or policy to agency owned Wi-Fi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handing procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents

involving mobile devices. This section lists three areas where enhanced incident handling and response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g., counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g., ask the question: "Is it reasonable to assume CJI could be accessed") as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a 'momentary' loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while 'minimal' durations might include a few minutes of time and 'extended' periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for

Wi-Fi only and on demand cellular devices, incident handling procedures that lock the device out of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on Wi-Fi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g., Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device with be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g., association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an 'always-on' cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in pace for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control **(CJIS Policy Section 5.5)**

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g., regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in 'general' purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g., phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control ***levels and access.***

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g., installing an application and accepting inappropriate security access levels for that application) my bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g., agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and required a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g., built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g., phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g., phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g., cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, Wi-Fi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device Wi-Fi Policy

Specific Wi-Fi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for Wi-Fi connections, however it was originally intended for defining requirements for fixed infrastructure Wi-Fi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal Wi-Fi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable Wi-Fi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g., Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a ‘trusted’ entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g., FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g., Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from 'general user' access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of 'routine' device functions which may be accessed by multiple individuals (e.g., phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g., PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

'Rooting' (Android OS) or 'Jailbreaking (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of 'traditional' anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a 'stock' Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with 'rooting' and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate 'secure' versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to 'unlock' the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g., phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g., secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full-featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the 'internal' storage of the device, the Android OS does not provide secure separation of data stores on 'external' storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific 'external' media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via 'always-on' cellular data connections and the devices built-in GPS. Device tracking with Wi-Fi only or 'on-demand' cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without 'always-on' cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a Wi-Fi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed Wi-Fi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g., GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full-featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed be means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local Wi-Fi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or "personal' firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may 'listen' on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating sys long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties

including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g., firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when

implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*

The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the

application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance:

Related control: IA-8.

(7) *LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*

The organization:

(a) Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) *LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*

The information system prevents [*Assignment: organization-defined software*] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6 (1) (2) (5) (9) (10)	**HIGH** AC-6 (1) (2) (3) (5) (9) (10)

SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS) CONSIDERATION FOR LEAST PRIVILEGE:

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving

to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the "20 Critical Security Controls for Effective Cyber Defense". This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled "Controlled Use of Administrative Privileges". SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12---1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	*Quick win (One of the "First Five")*
CSC 12---2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	*Quick win*
CSC 12---3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	*Quick win*

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	*Quick win*
CSC 12---5	Ensure that all service accounts have long and difficult--- to---guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	*Quick win*
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	*Quick win*
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	*Quick win*
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows "administrator" or UNIX "root" accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	*Quick win*
CSC 12---9	Configure operating systems so that passwords cannot be re---used within a timeframe of six months.	*Quick win*
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	*Visibility/ Attribution*
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	*Visibility/ Attribution*
CSC 12---12	Use multifactor authentication for all administrative access, including domain administrative access. Multi--- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	*Configuration/ Hygiene*

CSC 12---13 (NEW)	When using certificates to enable multi---factor certificate---based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	*Configuration/ Hygiene*
CSC 12---14	Block access to a machine (either remotely or locally) for administrator---level accounts. Instead, administrators should be required to access a system using a fully logged and non---administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	*Configuration/ Hygiene*

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes

delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g., a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements, but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

a. Separates [*Assignment: organization-defined duties of individuals*];

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption **–** A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption **–** A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption**.**

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality**.**

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

<u>Symmetric Encryption</u>

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

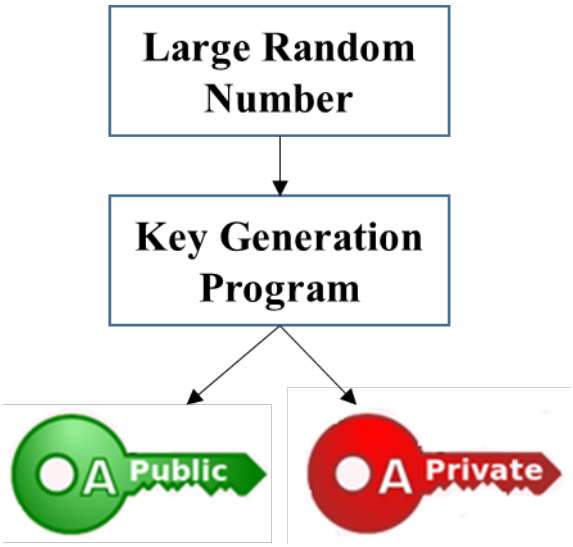


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality**.**

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

Symmetric		**Asymmetric**		
Bits of security	**Symmetric key algorithms**	**Finite-Field Cryptography (FFC) (e.g., DSA, D-H)** **Bits of security**	**Integer-Factorization Cryptography (IFC) (e.g., RSA)** **Bits of security**	**Elliptic-Curve Cryptography (ECC) (e.g., ECDSA)** **Bits of security**
80	2TDEA18	*Public key* = 1024 *Private key* = 160	*Key size* = 1024	*Key size* = 160-223
112	3TDEA	*Public key* = 2048 *Private key* = 224	*Key size* = 2048	*Key size* = 224-255
128	AES-128	*Public Key* = 3072 *Private key* = 256	*Key size* = 3072	*Key size* = 256-383
192	AES-192	*Public key* = 7680 *Private key* = 384	*Key size* = 7680	*Key size* = 384-511
256	AES-256	*Public key* = 15360 *Private key* = 512	*Key size* = 15360	*Key size* = 512+

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

> A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?
>
> • The module has been designed for compliance to FIPS 140-2. <NO>
>
> • Module has been pre-validated and is on the CMVP pre-validation list. <NO>
>
> • The module will be submitted for testing. <NO>
>
> • The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
>
> • The module meets all the requirements of FIPS 140-2. <NO>
>
> • The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
>
> • The module follows the guidelines detailed in FIPS 140-2. <NO>
>
> • The module has been validated and has received Certificate #XXXX. <YES>
>
> A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link: http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website: http://csrc.nist.gov/cryptval/140-2.htm

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a "living" document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the "Incident Response Life Cycle" as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



The initial phase of the incident response life cycle, "Preparation", involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection

and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident

- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- Functional Impact: the impact to business functionality
- Information Impact: the impact to confidentiality, integrity, and/or availability of criminal justice information
- Recoverability: the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e., malware) can exhibit several indicators. These indicators include, but are not limited to:

- Unexpected pop-up windows
- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of "ransom notes" on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user's perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers, firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection

and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and

ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave "recovery" instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines

many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e., a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
    - Preparation
    - Detection and Analysis
    - Containment
    - Recovery
    - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
    - Internal and external points of contact
    - Required tracking and reporting documents
    - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
    - Roles and responsibilities

- Incident-related information collection
- Updating policies with lessons learned
- Collection of evidence
- Incident response training
- Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce "in-house" software applications. By implementing security during the code writing process, security is "baked in" and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

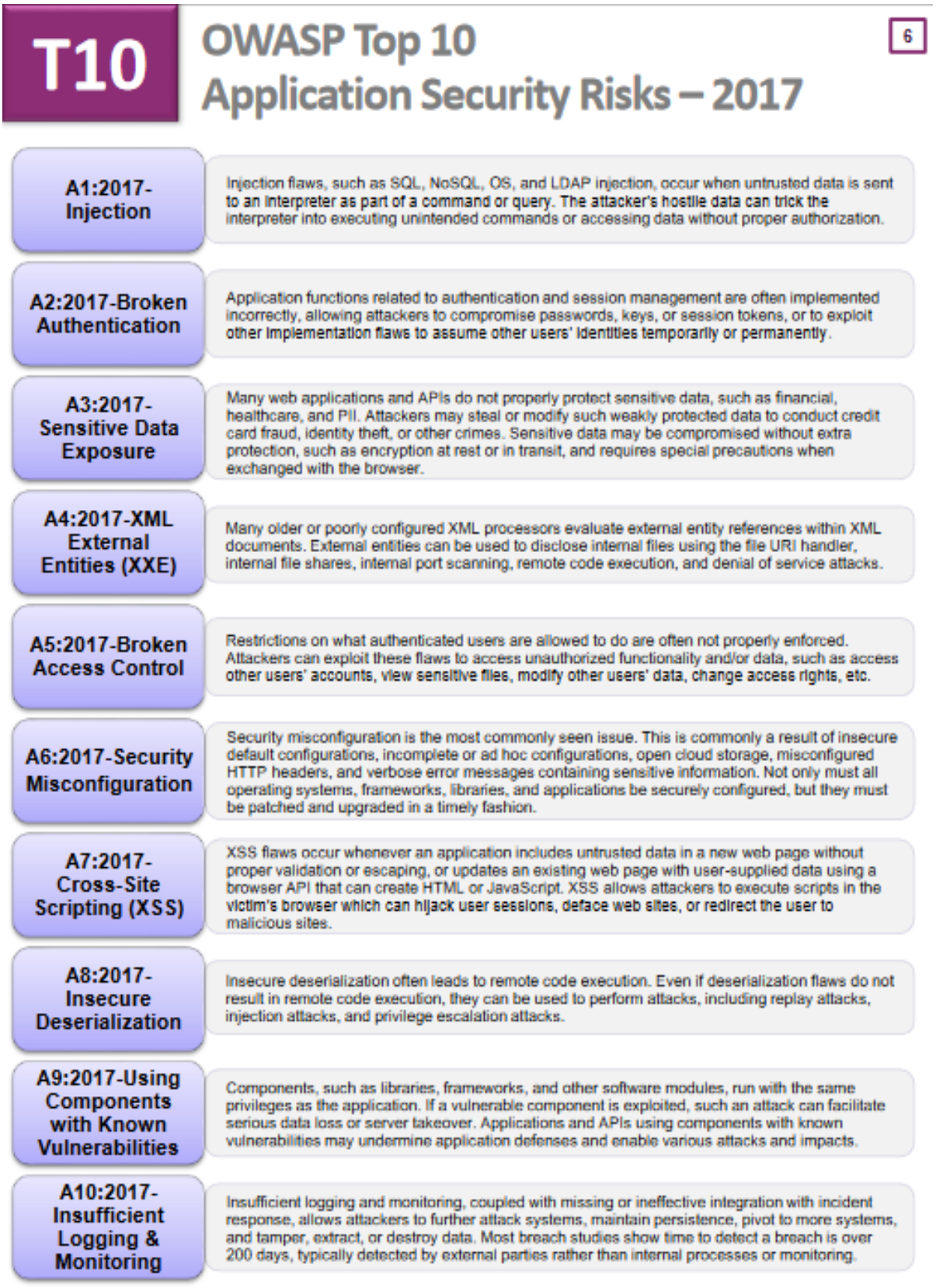
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A


T10
OWASP Top 10
Application Security Risks – 2017
6
A1:2017-Injection
Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication
Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure
Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)
Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-Broken Access Control
Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration
Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)
XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization
Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities
Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring
Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

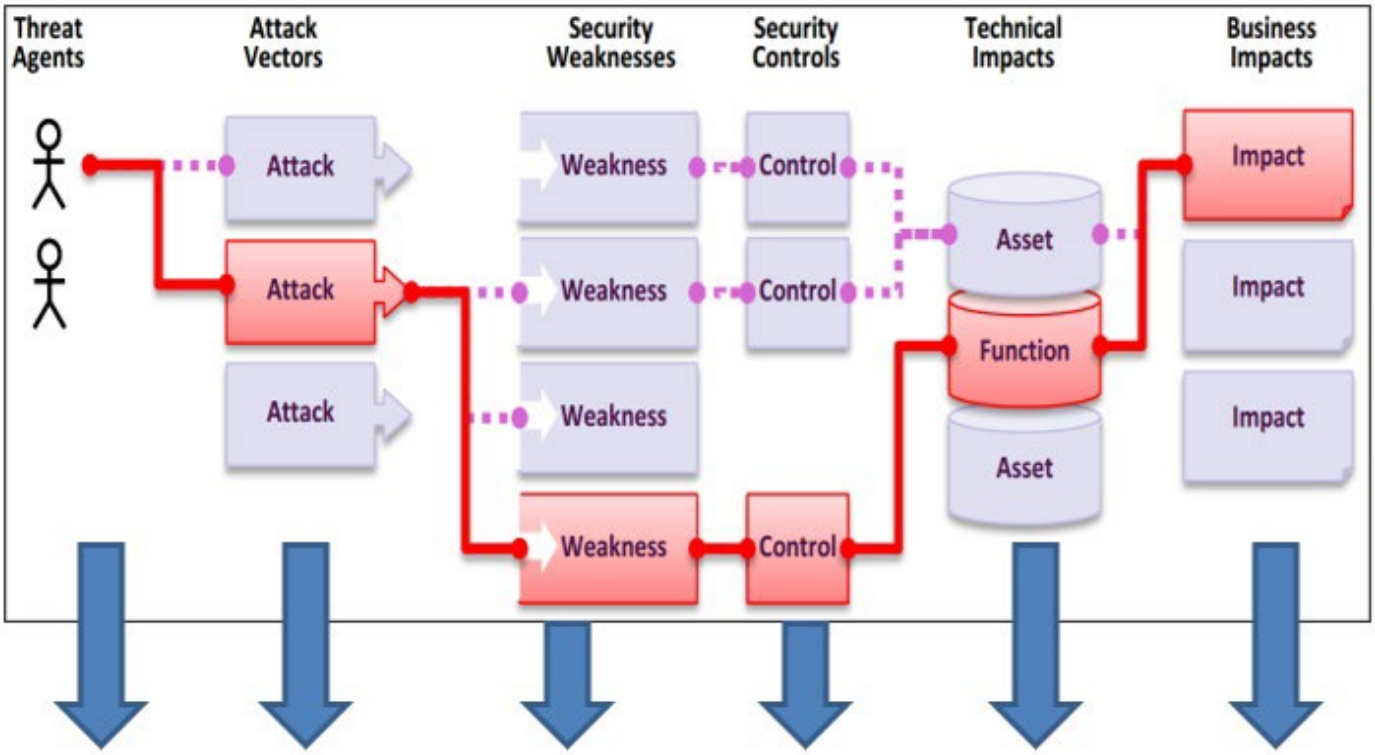
Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path



Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary

RISK	Threat Agents	Attack Vectors	Security Weakness		Impacts		Score
		Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere too.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
    - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- Application Security Verification Standard (ASVS):
  https://www.owasp.org/index.php/ASVS

- OWASP Secure Software Contract Annex:
  https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:
  https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):
  https://www.owasp.org/index.php/OWASP_SAMM_Project

- OWASP Application Security Guide for CISOs:
  https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:

  https://www.owasp.org/index.php/Category:OWASP_Education_Project

- OWASP WebGoat:
  https://www.owasp.org/index.php/WebGoat

- OWASP Broken Web Application Project:
  https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:
  https://www.owasp.org/index.php/OWASP_Testing_Project

- Application Security Verification Standard (ASVS):

  https://www.owasp.org/index.php/ASVS

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:
  https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- Application Security Verification Standard (ASVS): https://www.owasp.org/index.php/ASVS

APPENDIX H: SECURITY ADDENDUM

The following pages contain:

The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H-2-H-4);

An example of a contract addendum (H-5);

The Security Addendum itself (H-6-H-7);

The Security Addendum Certification page (H-8).

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

EXAMPLE OF A CONTRACT ADDENDUM

AMENDMENT NO. ___ TO THE CONTRACT BETWEEN
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. ___ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "___"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

a.

b.

c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _____, 20__.

On behalf of [Party No. 1]:

_____ _____
Printed Name Title

_____ _____
Signature Date

On behalf of [Party No. 2]:

_____ _____
Printed Name Title

_____ _____
Signature Date

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

APPENDIX I: REFERENCES

White House Memo entitled "Designation and Sharing of Controlled Unclassified Information (CUI)", May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of* 2002; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

[NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44

[NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2

[NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46

[NIST SP 800–48] *Wireless Network Security*: 802.11, *Bluetooth, and Handheld Devices*; NIST Special Publication 800–48

[NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52

[NIST SP 800–53] *Recommended Security* Control*s for Federal Information Systems*; NIST Special Publication 800–53, Revision 2

[NIST SP 800–53A] *Guide for Assessing the Security* Control*s in Federal Information Systems*, *Building Effective Security Assessment Plans*; NIST Special Publication 800–53A

[NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58

[NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT

[NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT

[NIST SP 800–64] NIST Special Publication 800–64

[NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act* (HIPAA); NIST Special Publication 800–66

[NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68

[NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70

[NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72

[NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1

[NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76

[NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77

[NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78

[NIST SP 800–81] *Secure Domain Name System* (DNS) *Deployment Guide*; NIST Special Publication 800–81

[NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

[NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86

[NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87

[NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96

[NIST SP 800–97] *Guide to* IEEE 802.11i: *Robust Security Networks*; NIST Special Publication 800–97

[NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121

[NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124

[NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125

[NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144

[NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145

[NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146

[OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996

[OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003

[OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006

[OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006

[OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006

[OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007

[Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004

[USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 – Government Agency and Employees, Part I – The Agencies Generally, Chapter 5 – Administrative Procedure,

Subchapter II – Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 – Public Printing and Documents; Chapter 35 – Coordination of Federal Information Policy; Subchapter I – Federal Information Policy, Section 3506

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2054: Good Neighbor Data Center Guidelines

ATTACHMENTS:

- Governor Letter Data Centers.pdf
- Data Center Guardrails.pdf

City of Charles Town

101 East Washington Street, P.O. Box 14, Charles Town, WV 25414
Phone: (304) 725-2311 ♦ Web: www.charlestownwv.us

October 14, 2026

The Honorable Patrick Morrisey
Governor of West Virginia
Office of the Governor
1900 Kanawha Boulevard, East
Charleston, West Virginia 25305

MAYOR
Micheal George

CITY COUNCIL

James Kratovil

Elizabeth Ricketts

Jeff Hynes

Kevin Tester

Nate Hartman

Alden Roth

Julie Smith

Andie Sugrue

CITY MANAGER

Alissa Meeks, Interim

Re: Jefferson County Good Neighbor Data Center Guardrails

Dear Governor Morrisey:

On behalf of the Charles Town City Council, we respectfully submit the attached Good Neighbor Data Center Guardrails and request these collective and locally developed protections be prioritized in the State's analysis of data center development impacting Jefferson County and local municipalities.

House Bill 2014 significantly restricts local government authority over impactful data center development. The associated guardrails attached reflect the community's thoughtful concerns, priorities, environmental considerations, and long-term character of our communities. Municipal governments are closest to the residents and businesses affected by major development decisions and our responsibility is to ensure that growth aligns with comprehensive plans, infrastructure capacity, and public safety needs. While these Good Neighbor Guidelines are a constructive step toward encouraging responsible data center development, HB 2014 significantly limits the ability of municipalities and counties to apply local control to data centers. As such, these current restrictions undermine the principle that communities should have a meaningful voice in determining how development occurs within local jurisdicitions.

Further, we are also concerned about the distribution of tax revenue generated by data centers as outlined in HB 2014. Under the statutory framework established by HB 2014, a portion of incremental tax revenue is distributed to the state and other designated recipients rather than remaining entirely within the jurisdiction where the development is located. The distribution formula raises legitimate questions about whether the communities bearing the direct impacts of development receive a proportionate share of the resulting public revenue and where the real associated development and impacts occur.

We appreciate your commitment to ensuring local input and we are confident that by collaboratively working together, West Virginia can welcome economic investment while simultaneously respecting local decision-making. We respectfully ask that your administration work with municipal leaders to revisit these concerns and pursue a more balanced approach to data center development.

Sincerely,

Micheal George,
Mayor

1. Protection of Groundwater Resources and Responsible Water Use

1.1 Managed Surface-Water Supply

Data centers in Jefferson County should obtain water through an existing public utility system supplied by a managed surface-water source, subject to confirmed utility capacity, reliability, treatment capability, and applicable regulatory approvals.

1.2 Groundwater Protection

Data centers should be prohibited from withdrawing groundwater directly, including through on-site wells, groundwater dewatering, or other groundwater-source systems, for cooling, domestic use, construction, fire-protection testing, irrigation, or other operational purposes.

1.3 No Indirect Groundwater Dependence

A data center should not rely on a public or private utility supply sourced from groundwater for normal operations. Any utility serving the facility should identify and document its water source and certify the extent to which its supply is derived from managed surface-water resources.

1.4 Reclaimed Water & Gray Water

Where technically feasible and authorized by applicable health, plumbing, environmental, and utility requirements, data centers should use reclaimed water, treated wastewater effluent, gray water, or other approved non-potable water sources for cooling towers, toilet flushing, irrigation, and other appropriate non-potable uses as the preferred use. Reuse systems must be properly designed, monitored, maintained, and protected against cross-connections, leaks, discharges, or seepage that could threaten public health or groundwater quality.

1.5 Low-Water Cooling Technology

Data centers should be required to use low-water or water-efficient cooling technology, including air-cooled, closed-loop, hybrid, direct-to-chip, or other demonstrably low-water systems. An applicant proposing a more water-intensive system should demonstrate that it provides equal or greater protection of local water resources and that no feasible lower-water alternative is available.

1.6 Water-Management Plan

Before approval, each applicant should submit a water-management plan identifying anticipated average and peak daily water demand; source or sources of water; proposed cooling technology; estimated annual water use; anticipated reclaimed-water, gray-water, wastewater generation; chemical-treatment practices; and potential effects on public-water capacity, wastewater capacity, streams, springs, wells, and groundwater resources.

1.7 Water Discharge Monitoring

Prohibit any unpermitted discharge of wastewater, process water, cooling water, fuel-contaminated runoff, chemicals, sediment, or other pollutants to surface waters, wetlands, drainageways, storm sewers, or groundwater. Data centers should be required to discharge all non-stormwater effluent to utilities with advanced treatment facilities such as CTUB. All onsite or offsite infrastructure required to treat effluent flows leaving the data center property and entering municipal owned system.

1.8 Wetlands and Marsh Protection

Data centers should not be located within wetlands, marshes, floodplains, or other environmentally sensitive areas. Data center should fund local watershed conservation and restoration efforts for the same water source that the cooling water is extracted from.

2. Protection of Air Quality and Public Health

2.1 Primary Use of Grid Power

Data centers in Jefferson County should be designed to operate primarily on electricity supplied through the regional electric grid.

2.2 Preference for Non-Combustion Backup Power

Where feasible, data centers should prioritize battery energy storage, redundant utility connections, and other non-combustion backup-power systems before relying on on-site fuel-fired generators. Backup systems should be designed to minimize air emissions, noise, fuel storage, traffic, and risks to neighboring residents and prioritize natural gas over diesel when available.

2.3 Major-Source Air-Permit Review

Every proposed data center should complete a comprehensive air-emissions assessment before County approval. Where projected emissions meet the legal threshold for a major source, the applicant must obtain all applicable major-source permits, including Prevention of Significant Deterioration or other New Source Review authorization, before construction or operation.

2.4 Best Available Emission Controls

Applicants should use the best available air-emissions control technology and operational practices appropriate to the facility. The analysis should evaluate cumulative emissions from all generators, boilers, cooling equipment, construction activity, delivery traffic, and other on-site emission sources, rather than considering each engine or source in isolation or phase of project.

2.5 Public Notice, Comment, and Hearing

All air-permit applications, emissions analyses, and supporting technical studies should be publicly available. Projects with significant emissions, substantial community interest, or potential effects on nearby homes, schools, farms, health-care facilities, or sensitive

environmental resources should be subject to a meaningful public-comment period and a locally accessible public hearing.

2.6 Responsible Outdoor Lighting Using Dark-Sky Standards

Comply with international illumination dark-sky standards.

3. Stormwater Management and Soil-Contamination Mitigation to Corresponding Local Jurisdiction

3.1 Stormwater and Drainage Protection

Jefferson County should require major data centers and other large-scale developments to protect neighboring properties, public infrastructure, streams, and water resources from stormwater impacts during construction and throughout the life of the project.

3.2 Independent Plans and Effective Controls

Applicants must submit independently reviewed stormwater, drainage, grading, and erosion-and-sediment-control plans. Effective controls must be installed and maintained before land disturbance begins, and construction should be phased to reduce exposed soil and unmanaged runoff.

3.3 No Increased Downstream Impacts

Applicants must demonstrate that the proposed development will not increase flooding, erosion, sedimentation, or drainage impacts on downstream properties, public roads, streams, springs, or other water resources.

3.4 Inspection, Enforcement, and Financial Assurance

The County should retain authority to conduct enhanced inspections, require immediate corrective action, and issue stop-work orders when stormwater or erosion-control measures fail. Applicants should provide adequate financial assurance so that cleanup, repairs, restoration, and project-related damages are paid by the developer—not residents or taxpayers.

4. Local Staff and First-Responder Safety Review

4.1 County and Fire-Rescue Review

Jefferson County should require major data centers and other large-scale developments to provide County staff and the local first-due fire station with a safety and operational review before construction begins and again before occupancy.

4.2 Required Safety Information

The review should address site access, building layout, fire-protection systems, water supply, hydrant locations and fire flow, utility shutoffs, fuel and battery systems, hazardous materials, emergency communications, and anticipated emergency-response needs.

4.3 Pre-Incident Planning and Developer Responsibility

Applicants should complete reasonable safety measures identified by local responders, including pre-incident planning, site walk-throughs, emergency drills, training, equipment evaluation, access improvements, and mutual-aid coordination. The applicant should bear the reasonable costs of project-specific planning, training, equipment, and mitigation measures necessary to safely serve the facility.

Noise, Setbacks, and Vegetative Screening			
Property Type	**Noise (dBA) Maximum**	**Setbacks (site & building)**	**Vegetative Screening**
Industrial Use or Zone	70 dBA	50 ft minimum	Minimal buffer along side and rear; complete buffering along frontage for 8-10 minimum height planting
Commercial Use or Zone	65 dBA	100 ft minimum	A mixture of plantings that is predominantly evergreen, 6-foot minimum height at planting. Complete buffering and screening required.
Agricultural/Residential Use or Zone	55 dBA	1,000 ft minimum	A mixture of plantings that is predominantly evergreen that is non-invasive with goal of providing native and/or hybrid native, 8–10-foot minimum height at planting. Staggered multi-layers as appropriate Complete buffering and screening required. Consider design factors such as walls or landscape to limit visual disturbance.
Institutional Use/Zone (schools, churches, etc.)	60 dBA	1,000 ft minimum	A mixture of plantings that is predominantly evergreen that is non-invasive with goal of providing native and/or hybrid native, 8–10-foot minimum height at planting. Staggered multi-layers as appropriate Complete buffering and screening required. Consider design factors such as walls or landscape to limit visual disturbance.
Any Historic Designation Property	55 dBA	1,000 ft minimum (from historic structure)	A mixture of plantings that is predominantly evergreen that is non-invasive with goal of providing native and/or hybrid native, 8–10-foot minimum height at planting. Staggered multi-layers as appropriate Complete buffering and screening required. Consider design factors such as walls or landscape to limit visual disturbance.

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2055: Depot Land Memorandum of Understanding (MOU) with Charles Town Parks and Recreation Commission

ATTACHMENTS:

- Depot District Memorandum of Understanding_Draft 2.pdf

MEMORANDUM OF UNDERSTANDING

Between the Charles Town City Council and the Charles Town Parks and Recreation Commission Regarding the Depot District

This Memorandum of Understanding (the **MOU**) is entered into as of the date of the last signature below (the **Effective Date**) by the **Charles Town City Council**, acting on behalf of the **City of Charles Town, West Virginia** (the **City**), and the **Charles Town Park and Recreation Commission** (the **Commission**). The City and the Commission are referred to collectively as the **Parties**.

Recitals

The City acquired certain land from American Public University System on February 14, 2024, by deed identified as recorded in Deed Book 1340 at page 468 (the **Depot District** or **Property**). The Parties understand that the Property is currently vacant. The deed's legal description, rather than the shorthand name "Depot District," controls the identification of the Property under this MOU.

The City desires that the Property function as both a civic space for the community and an economic development space that can support appropriate public programming and activity. The Parties desire to coordinate the Property's planning, day-to-day use, and maintenance while preserving the City's ownership and governmental authority.

Accordingly, the Parties agree as follows:

Understanding

1. Purpose and guiding uses. The Parties will work together to make the Depot District a welcoming, accessible civic gathering place and a venue for activities that support local economic vitality. Uses may include public gatherings, cultural and recreational programming, community markets, and other temporary activities consistent with applicable law, site conditions, public safety, and City-approved plans. This MOU does not itself approve any particular event, construction project, lease, concession, or exclusive use.

2. Ownership and reserved authority. Title to the Property remains with the City. Nothing in this MOU conveys a real-property interest, grants exclusive possession, or limits the City's authority over land use, capital development, public improvements, economic development policy, or disposition of the Property. The Commission will act only within its lawful authority and the scope of approvals and resources made available by the City.

3. Parks and Recreation Master Plan. The City Council has allocated $75,000.00 to the Commission for preparation of the Parks and Recreation Master Plan generally, including an

additional $25,000.00 previously allocated for a study of the Depot District property. That additional $25,000.00 will be available to the Commission for preparation of the Master Plan generally, rather than solely for a separate study of the Property. Use of the allocated funds remains subject to lawful appropriation, applicable purchasing requirements, and approval by the responsible body under Section 7.

The Commission will include the Depot District in the next adoption or update of the Parks and Recreation Master Plan, expressly identifying its dual civic-space and economic-development purposes. The Commission will coordinate the proposed treatment of the Property with the City and receive City Council approval before submission or adoption of the plan, and will reflect City-approved priorities for public access, programming, maintenance, and future improvements. Inclusion in the plan does not independently authorize spending or development.

4. Day-to-day operations and coordination. Subject to applicable law, available appropriations, and the City's retained ownership and authority under Section 2, the Commission will control the Property's day-to-day operations, including routine scheduling, public programming, ordinary grounds care, and administration of public use. Event scheduling, programming, and use are subject to Section 5 and the City's Special Activity Permit Policy (the Policy). The Commission may make ordinary operating decisions without separate City approval where those decisions comply with this MOU and applicable City requirements, including but not limited to the Policy The City will designate a representative from its economic development staff to coordinate with the Commission on economic-development uses, event planning, infrastructure, and any planned changes to the site. The Commission may carry out routine grounds care and coordinate proposed programming, but the Policy and other applicable City procedures govern authorization of public events and third-party use.

5. Events and third-party use. Events at the Property will be handled in accordance with the City of Charles Town Special Activity Permit Policy (the Policy), effective March 3, 2025, as amended by the City. The Policy governs permit requirements, applications, review and approval, fees and charges, conditions of approval, insurance and hold-harmless requirements, changes to approved activities, cancellations, revocations, appeals, and post-activity evaluation, as applicable. If this MOU or the operating plan conflicts with the Policy concerning event permitting or approval, the Policy controls.

The Commission will plan and manage recreational and civic events at the Property subject to the Policy and the approved operating plan, and will coordinate its event calendar and planning with the City's economic development staff, particularly for events intended to support local businesses, tourism, markets, or other economic-development objectives. The Commission and City staff will consult in advance on proposed events that materially affect the other's planned use, require City services or resources, or implicate economic-

development commitments. Scheduling conflicts will be addressed through coordination and the Policy's review and approval process, including its requirements concerning interference with previously approved or scheduled activities.

Applicants must obtain all permits and approvals required by the Policy before conducting an event. Special Activity Permits will be reviewed and approved or denied by the City Manager, with consultation, additional approvals, referrals, and appeals handled as provided in the Policy. Neither Commission approval, inclusion on an event calendar, nor approval of any operating plan substitutes for a required Special Activity Permit or other governmental approval.

Any vendor arrangement, sponsorship, concession, rental, license, or other third-party occupancy requiring a contract or governmental approval must be separately authorized by the City and, where applicable, the Commission. No Party may bind the other to an expenditure, contract, or event commitment without that Party's authorized written approval. Uses must comply with applicable law and any City rules, permits, and nondiscriminatory public-access requirements.

6. Improvements and site work. The Commission will not undertake permanent construction, alteration, demolition, excavation, or installation of fixed improvements on the Property under this MOU alone. Any such work requires a the City to separately approve scope, budget, allocation of responsibility, and any necessary permits or other approvals. The City retains control over decisions concerning permanent improvements and future redevelopment, after consultation with the Commission concerning recreational and civic uses.

7. Funding and risk management. Each Party bears its own costs under this MOU unless the Parties separately approve a written funding arrangement. All expenditures remain subject to lawful appropriation, purchasing requirements, and approval by the responsible body. This MOU does not create an indemnity or waive any governmental immunity or defense available under law.

8. Coordination and review. The Parties will designate points of contact and meet at least annually to review the Property's condition, public use, programming, economic-development opportunities, and any proposed revisions to the Master Plan or operating plan. Each Party will promptly notify the other of a material safety issue or proposed activity that could materially interfere with the other Party's planned use.

9. Term; amendment; termination. This MOU begins on the Effective Date and continues until terminated by either Party on thirty (30) days' written notice, or earlier by mutual written agreement. Either Party may suspend activities under its control immediately to address an imminent safety concern or legal requirement, with prompt

notice to the other Party. Any amendment must be in writing and approved by both Parties through their respective authorized processes. Termination does not affect City ownership or any independently executed agreement with a third party.

10. Nature of MOU. This MOU records the Parties' intended allocation of planning and operating responsibilities; it does not create a separate legal entity or authorize either Party to act beyond its legal powers. If an existing ordinance, charter provision, deed restriction, grant condition, or other binding requirement conflicts with this MOU, that requirement controls, and the Parties will confer on a conforming amendment.

Approval and signatures

The undersigned sign on behalf of their respective bodies after any required authorization.

CHARLES TOWN CITY COUNCIL, on behalf of the City of Charles Town

By: _____ Date: _____

Michael George, Mayor

CHARLES TOWN PARK AND RECREATION COMMISSION

By: _____ Date: _____

Alden Roth, Chair

DRAFT

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2008: TXA2026-01 - Flood Control Ordinance - First Read

ATTACHMENTS:

- 1. Report.pdf
- Floodplain Resolution Draft.pdf

Date: For the October 19, 2026 City Council meeting
From: James Newman, City Planner, Zoning/Subdivision Administrator

FLOOD CONTROL – Proposed Change

A. Background

Starting in 2023, the Federal Emergency Management Agency (FEMA) began work on updating flood maps for Jefferson County, including Charles Town. As part of this process, the City is required to update its Flood Control Standards. The current standards are in Article 1741 'Flood Control' of the City's Codified Ordinances.

B. Current Standards - Applicability

1741.01.D. "Applicability. This article shall apply to all lands within the City of Charles Town that are subject to the One Hundred (100) Year Flood as shown on the Flood Insurance Rate Map (FIRM) and described in the Flood Insurance Study (FIS) prepared for the City of Charles Town by the Federal Emergency Management Agency (FEMA) dated December 18, 2009, or the most recent revision thereof."

C. Map Change

FEMA issued public notice of map changes on August 14, 2025, with a 90 day appeal period running to November 12, 2025. Notice was given in the Spirit of Jefferson, Federal Register, FEMA sponsored radio/tv/social media notice, and City of Charles Town social media feeds and public bulletins. No appeals were filed. The revised Flood Insurance Study and Flood Insurance Rate Maps will become effective November 27, 2026.

D. State Review

As part of this process I contacted the State's National Flood Insurance Program Coordinator to review our existing Flood Control Ordinance to see if it is up to date or needs revisions. I received the following response:

I did review your ordinance and it is perfectly fine to keep it as it, with this exception: The change that will need to be made is in Section 1741.01 General Provisions Subsection (d): the date of your news maps will be November 27, 2026 (the date you have in there now is December 18, 2009.) --- Julia Sears, CFM, NFIP/CTP Coordinator, WV Emergency Management Division, delivered via email Sept. 4, 2026.

E. Council Action

Council voted unanimously to start the public hearing process at their October 5, 2026 meeting.

F. Request

Council should vote to approve the first read to amend the Codified Ordinances of the City of Charles Town Part 17, Chapter 3, Article 1741.01.D. to read:

"Applicability. This article shall apply to all lands within the City of Charles Town that are subject to the One Hundred (100) Year Flood as shown on the Flood Insurance Rate Map (FIRM) and described in the Flood Insurance Study (FIS) prepared for the City of Charles Town by the Federal Emergency Management Agency (FEMA) dated **November 27, 2026,** or the most recent revision thereof." (Changed text **bolded**)

A RESOLUTION OF THE CITY OF CHARLES TOWN, WEST VIRGINIA, ACKNOWLEDGING AND ADOPTING REVISIONS TO THE FEMA FLOOD INSURANCE RATE MAPS (FIRMs) AND AUTHORIZING AMENDMENTS TO THE LOCAL FLOODPLAIN MANAGEMENT ORDINANCE.

WHEREAS, the City of Charles Town ("City") participates in the National Flood Insurance Program (NFIP) administered by the Federal Emergency Management Agency (FEMA); and

WHEREAS, to maintain eligibility for flood insurance and federal disaster assistance for property owners within the jurisdiction, the City must adopt and enforce a compliant floodplain management ordinance that reflects current, accurate flood hazard data; and

WHEREAS, FEMA has issued Final Map Revisions to the Flood Insurance Rate Maps (FIRMs) and/or Flood Insurance Study (FIS) report for Jefferson County, West Virginia and the City of Charles Town, with an effective date of November 27, 2026; and

WHEREAS, West Virginia Code and the [City/Town/County] Floodplain Management Ordinance require the local governing body to officially acknowledge changes to physical boundaries or flood hazards and incorporate updated digital or physical data into its official zoning and floodplain maps; and

WHEREAS, the City finds that adopting these revised flood maps is necessary to promote the health, safety, and general welfare of the citizens of Charles Town and to minimize future flood losses.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF CHARLES TOWN, WEST VIRGINIA:

1. **Acknowledgment and Adoption:** The City hereby formally acknowledges, accepts responsibility for enforcing, and adopts the revised FEMA Flood Insurance Rate Map (FIRM) panels and accompanying Flood Insurance Study (FIS) text updates effective November 27, 2026, as the official regulatory flood data for local permitting and spatial planning.

2. **Ordinance Integration:** The local Floodplain Administrator is directed to update the official references within Section 1741.02 of Article 1741 of the Charles Town Flood Control Ordinance to reflect the newly adopted effective dates.

3. **Public Record:** The revised map boundaries, Base Flood Elevations (BFEs), and floodway determinations shall be maintained on file for public inspection at City Hall.

DRAFT

4. **Federal Notification:** The Floodplain Administrator is authorized and directed to notify the FEMA Region III Office and the West Virginia State Coordinating Agency (West Virginia Floodplain Management Program) in writing of this adoption to maintain active status in the NFIP.

ADOPTED this _____ day of _____, 2026.

Attest:

_____ _____

Michael George
Mayor

Alissa Meeks
City Clerk

DRAFT

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-1989: Walkability Improvement Grant - Updates

The Infrastructure Committee recommends continuing to assess opportunities for revamping the Walkability Improvement Grant Program, but in the meantime, recommends the program be updated to:

i. Increase the amount for each award for inflation to $7,000
ii. Add design detail for brick sidewalks into the standards which
will require a concrete base and proper curbs.
iii. Allow corner lots with two sidewalk sections to apply for a double award.
iv. Remove language in the grant prohibiting brick where it does not already exist.

ATTACHMENTS:

- 1. Staff Report.pdf
- 2. WIP Application- CURRENT.pdf
- 3. WIP Application- DRAFT Version with changes.pdf

Date: For the October 19, 2026 City Council meeting
From: James Newman, City Planner, Zoning/Subdivision Administrator

Walkability Improvement Grant – Proposed Changes

1. **Walkability Improvement Grant – Current Parameters**

   This grant is handled administratively by the Zoning Administrator; no public hearings or board/commission/Council meetings or approvals are required. The purpose of the grant is to "*improve and enhance the overall pedestrian experience in Charles Town*", by helping to finance the restoration, repair sidewalks, as well as the creation of new sidewalks for properties with a building(s) but no sidewalk.

2. **Infrastructure Committee**
   The Infrastructure Committee reviewed this item at their meetings on September 17 and October 1, 2026. Following an overview of the grant program and proposed changes by myself and the Code Enforcement Officer, the Committee recommended:

   A. Increase the payment cap from $5,000 to $7,000 to keep up with inflation.

   B. Allow for corner lots to access up to $14,000, as these lots have multiple sidewalks.

   C. Permit both brick and concrete as acceptable materials.

   D. Added in brick sidewalk standards.

3. **Changes in the Draft Version**

   A. Increase the payment cap from $5,000 to $7,000 to keep up with inflation.

   B. Allow for corner lots to access up to $14,000, as these lots have multiple sidewalks.

   C. Permit both brick and concrete as acceptable materials. Currently brick is only allowed to replace existing brick. This change allows for new brick sidewalks to be installed.

   D. Added in brick sidewalk standards, as well as curb and gutter standards.

   E. Changed diagrams to require *Americans with Disability Act* compliant designs.

   F. General reformatting.

4. Recommendation

Approval of the proposed changes.

CITY OF CHARLES TOWN
WALKABILITY IMPROVEMENT PROGRAM







City of Charles Town
101 East Washington Street
Charles Town, WV 25414

Phone: 304-724-3248
Website: www.charlestownwv.us

Investing in the Future of Charles Town

Charles Town's Walkability Improvement Program was designed as an effort to improve and enhance the overall pedestrian experience in Charles Town. The program is intended to assist applicants in improving the quality of the sidewalks along their property. Improved sidewalks provide safe, accessible streets for all residents, and promote walkability. These benefits contribute to the goals within the comprehensive plan to improve pedestrian experience and quality of life. Approved applicants in this program are eligible to receive financial assistance of **50/50 matching funds** for sidewalk repairs or installation, of up to $5,000.00. The program is managed by the City Staff. The program components may be amended periodically to accommodate new or modified City policies and procedures.

Policy for Two Bids:

1. **Two Bids** will be required for any application submission.
2. If the work is to be completed by the property owner, verification of expenses by a bid or a website such as homewyse.com will be required.

Policy for Walkability Improvement Program Expiration Date:

1. After an award of a Walkability Improvement Program Grant, the awardee will have one year from the time of the award to complete the improvements.

PROGRAM ELIGIBILITY

All sidewalks in the City of Charles Town are eligible in the program. Highest priority to properties with gaps. Sidewalks that are in poorest condition will be given higher priority. Existing buildings without sidewalks are also eligible. The following matrix which is from the Charles Town Walkability and Connectivity Study will be used to identify sidewalks that need the most improvement.

For an application in which the sidewalks are not identified in the Walkability and Connectivity study, the evaluation of the application will be by the same standards by which the Walkability and Connectivity study was created.

Priority	Wide Assessment	Condition Assessment
1	Poor	Poor
2	Fair	Poor
3	Poor	Fair
4	Good	Poor
5	Poor	Good
6	Fair	Fair
7	Good	Fair
8	Fair	Good
9	Good	Good

CITY OF CHARLES TOWN
WALKABILITY IMPROVEMENT PROGRAM

ELIGIBLE PROJECTS

The only permissible material approved for the Walkability Improvement Program is concrete or brick. Brick is only permitted where there are existing brick sidewalks. Existing buildings with no sidewalk are eligible for the grant as well.

INELIGIBLE PROJECTS

New construction projects, government properties, and national franchise properties are not eligible to participate in the Walkability Improvement Program. Private walks extending from the street curb to the main sidewalk and private service walks extending from the main sidewalks to the home or business are the sole responsibility of the owner.

Ineligible projects may be considered for approval at the discretion of City Council at their first meeting in June, provided no eligible project applications have been received by close of business on the first working day of June.

SIDEWALK WIDTH

All sidewalks shall be a minimum of 5 feet wide, unless constraints on the property do not permit this width. Most sidewalks in the City are not 5 feet wide. This program will require those sidewalks to be widened. It is known that there are a few limited locations in the City, that this cannot be achieved. City staff will examine each request and make a determination regarding the ability to install the 5-foot-wide sidewalk.

SURVEY

Where sidewalks do not exist, a survey will be required to ensure that sidewalks are located along the edge of the right-of-way. Survey will be an eligible reimbursement.

APPLICATION PROCESS

Each applicant will be eligible to apply up to $5,000.00 each fiscal year. The applicant shall complete and submit the Walkability Improvement Program Application to include the following:

- Proposal, estimates, sketches/photographs, and a written, detailed description of the project to be considered for the matching grant;
- Applicants are expected to complete the 50% matching portion of the estimated project cost and submit proposed/estimated cost in the application. A **minimum of two bids** must be provided; and
- Grant Approval Agreement will be signed by the property owner.

CONDITIONS OF APPROVAL

In addition to previously listed requirements:

- all properties must be current to date on all municipal taxes;
- each property will be eligible for one application per twelve (12) month period
- grants may be limited based on availability; and
- Applicant are encouraged to have read the Charles Town Walkability and Connectivity Study.

APPROVAL PROCEDURES

Each application will be reviewed, and the property will be deemed eligible or ineligible for grant funding by staff. If deemed eligible, staff will make a decision based on compliance of the project with the Charles Town Walkability and Connectivity Study and the Ordinances of the City of Charles Town. If the application is denied, the applicant will receive notification and an explanation of the denial. The City may also provide recommendations for modifications that could be made for the project to receive consideration for approval at a future funding cycle.

APPROVED PROJECT

The City will contact the applicant and the following shall occur:

- applicant may begin his/her matching portion of the project.
- apply for and obtain all necessary permits.
- submit receipts/invoices to the City once the project is complete for reimbursement.

Construction may begin only after the application has been approved and an agreement has been signed. **Any work completed prior to formal written approval will not be eligible for the match funding.**

PROJECT MANAGEMENT

All applicants accepted into the Walkability Improvement Program will be fully responsible for managing construction of projects, including, but not limited to, obtaining bids, selecting contractors, obtaining approvals, permits, and insurance, overseeing construction work, and paying all invoices for work, materials, and supplies. Any contractor or subcontractor must have a valid business license issued by the City of Charles Town. The applicant is responsible for ensuring that all contractors and subcontractors meet these requirements.

The City of Charles Town encourages employment and business opportunities for local residents and businesses. Applicants should seek to solicit bids and proposals, materials, and labor from qualified local residents and businesses whenever possible.

CITY INSPECTION PROCESS

1. Installation of forms
2. Post pour Inspection
3. Back fill

NON-DISCRIMINATION - EQUAL EMPLOYMENT OPPORTUNTY

Applicants shall follow the City's non-discrimination ordinance and equal employment opportunity requirements in the solicitation of contractors, subcontractors, workers, and suppliers.

CITY ACCOUNTABILITY

The City's participation in this program does not make the city liable regarding the quality and/or soundness of construction or other repairs, additions, or removals. Any contractor or subcontractor working on the project must be licensed and insured.

PAYMENT OF MATCHING FUNDS

Upon completion of the project, the Applicant will provide accounting of all project costs and a copy of all paid invoices. Projects must be completed within twelve (12) months after formal approval has been granted. Any time extension must be filed and approved by staff.

Reimbursement will be issued after the property owner's portion of the project has been completed, including site inspections and the City has received receipts detailing the completed work. If the project meets all standards, the City will provide funding for no more than the amount awarded in the grant application.

APPLYING AS A TENANT

Tenants applying for the Walkability Improvement Program shall have the property owner's permission to make any improvements detailed in this application. The property owner of record signature shall be required on all applications and no application will be accepted if the property owner signature is not present.

ADDITIONAL INFORMATION

The City recommends that any applicant(s) interested in applying for acceptance into the Walkability Improvement Program contact City staff prior to submitting an application. Questions about the program may be directed to the City Planner. Applications may be obtained at City Hall and at www.charlestownwv.us.

CITY OF CHARLES TOWN
WALKABILITY IMPROVEMENT PROGRAM

APPLICATION

No application fee applies

1. Applicant's Name: _____ Date: ____/____/____
Day Month Year

2. Mailing Address: _____

3. Project Address: (if different from mailing) _____

4. E-mail: _____ 5. Phone: _____

6. Contractor Address: _____, _____, _____

7. Company Name: _____ 8. Phone: _____

9. Sidewalk details
☐Front yard ☐Side-yard ☐ADA ramps

Projects that answer yes to any of the following questions are not eligible for the program:

10. Has the property in this application been awarded a Sidewalk Improvement Program grant in the past 12 months?

☐ Yes ☐ No

11. Is this property:

New construction? ☐ Yes ☐ No

Government-owned property? ☐ Yes ☐ No

A national franchise? ☐ Yes ☐ No

12. Description of the Walkability Improvement project:

13. Estimated Project Start Date: _____/_____/_____ (Day / Month / Year)
14. Estimated Project Completion Date: _____/_____/_____ (Day / Month / Year)

15. Estimated Total Project Budget: _____

16. Grant Amount Requested: _____

17. The following items are included with this application:

- ❑ Existing condition photographs
- ❑ Detailed proposal and/or contractor estimates
- ❑ Charles Town Walkability and Connectivity study

18. I have reviewed the following documents:

- ❑ Codified Ordinances of the City of Charles Town
- ❑ Construction Details for Sidewalks

Upon approval of the application the following will be required by the applicant:

- obtain all necessary building permits
- pass City inspection of improvements to ensure compliance with the sidewalk construction details and intended outcomes based on the funding application submittal
- submit receipts/invoices to the City upon completion of the project

I agree that the information provided above and within is accurate and correct to the best of my knowledge. I also assure that the property listed is in compliance with all laws, ordinances, rules, and regulations of the State of West Virginia and the City of Charles Town.

Applicant's Printed Name: _____

Signature of Applicant: _____

Signature of Property Owner(s) (if different than applicant): _____

Date of Application: _____/_____/_____ (Day / Month / Year)

FOR CITY USE ONLY

Application Number:_____ Date Application Received:_____

Approved:_____ Date:_____

Comments:_____

_____

Grant Approval Agreement

1. **I agree to follow the plan submitted with the application and I understand that failure to do so may disqualify the project for grant funding.**

2. **I agree to complete all improvements within one year of approval from the approval of the grant. Any time extension must be filed and approved by Staff.**

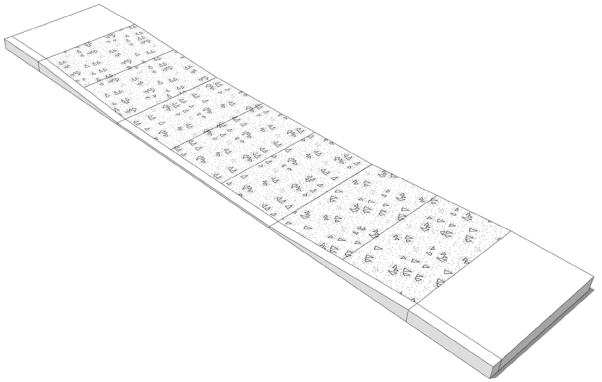
3. **I agree to all of the attached "Conditions of Approval", if any.**

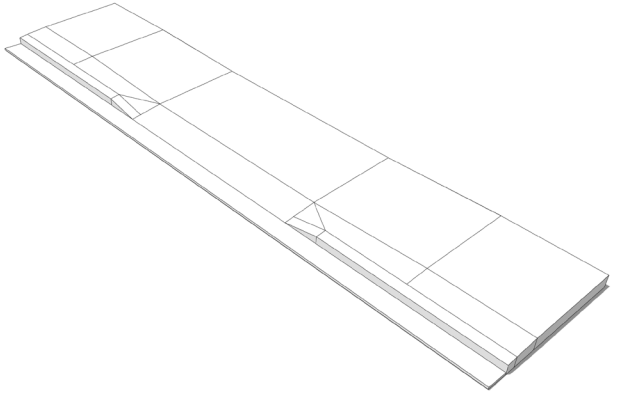
4. **I understand that I have to provide receipts related to the project. If a contractor was used, a written invoice must be provided to the City before funds will be granted. For projects that involve a contractor, receipts and invoices must be accompanied by proof of payment (i.e. cancelled checks). If a contractor was not used, receipts must be provided to the City Staff before a reimbursement will be issued. Only materials may be reimbursed for projects that do not use a contractor. Receipts and invoices must be accompanied by proof of payment.**

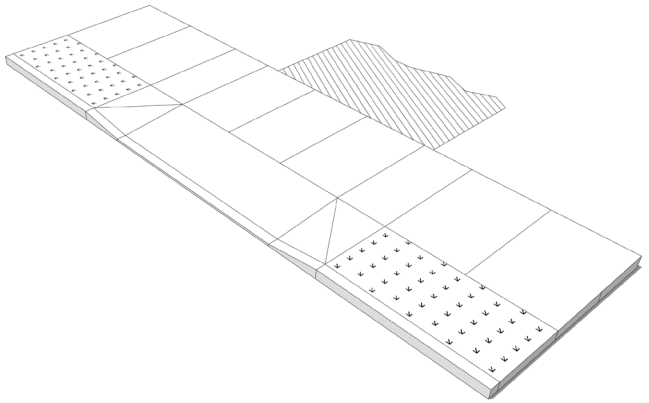
5. **I understand that grant monies shall not be distributed until all proposed work is completed and has passed inspected.**

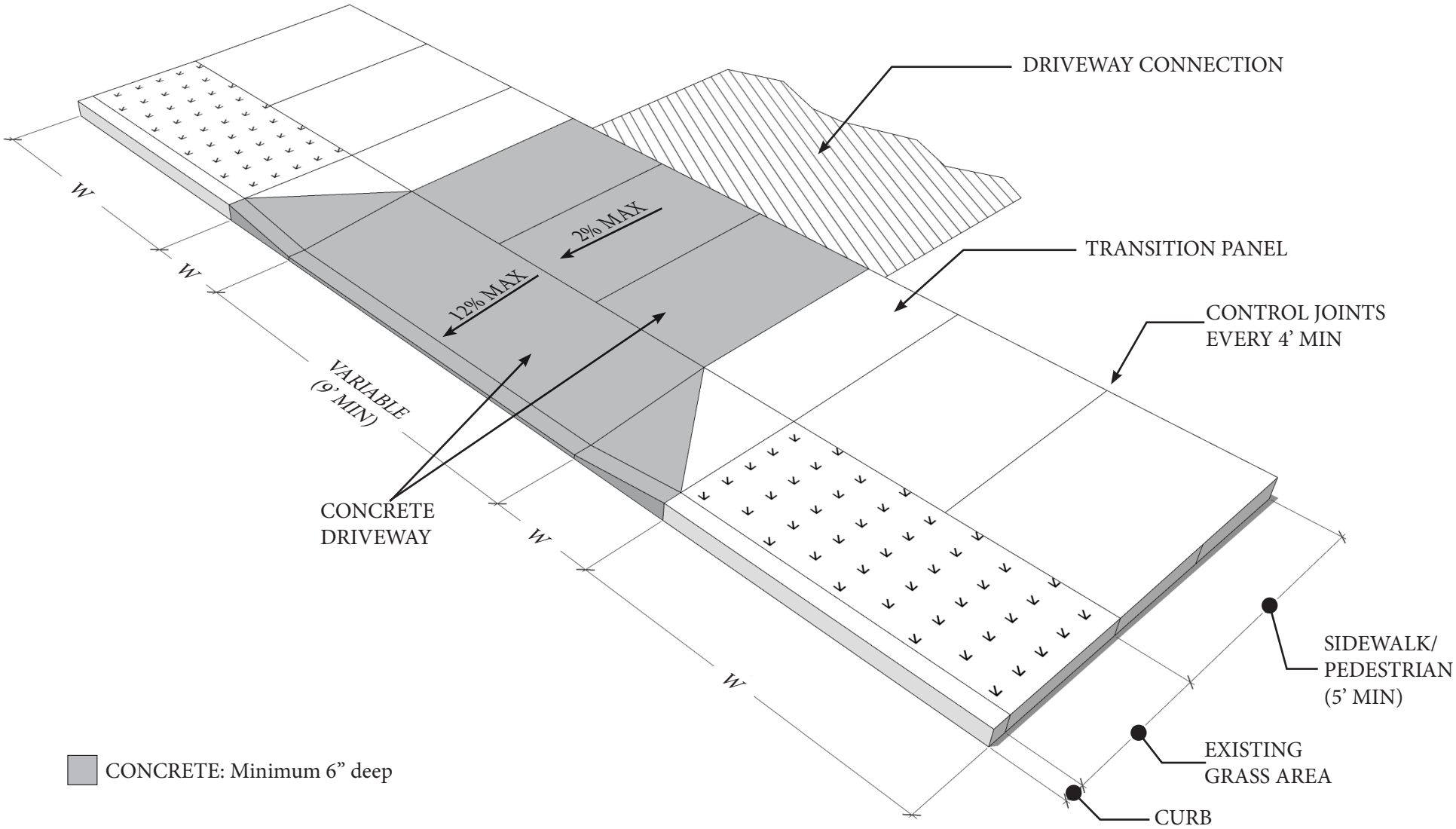
Property Owners Signature _____ **Date** _____

SIDEWALK
IMPROVEMENT
STANDARD DETAILS



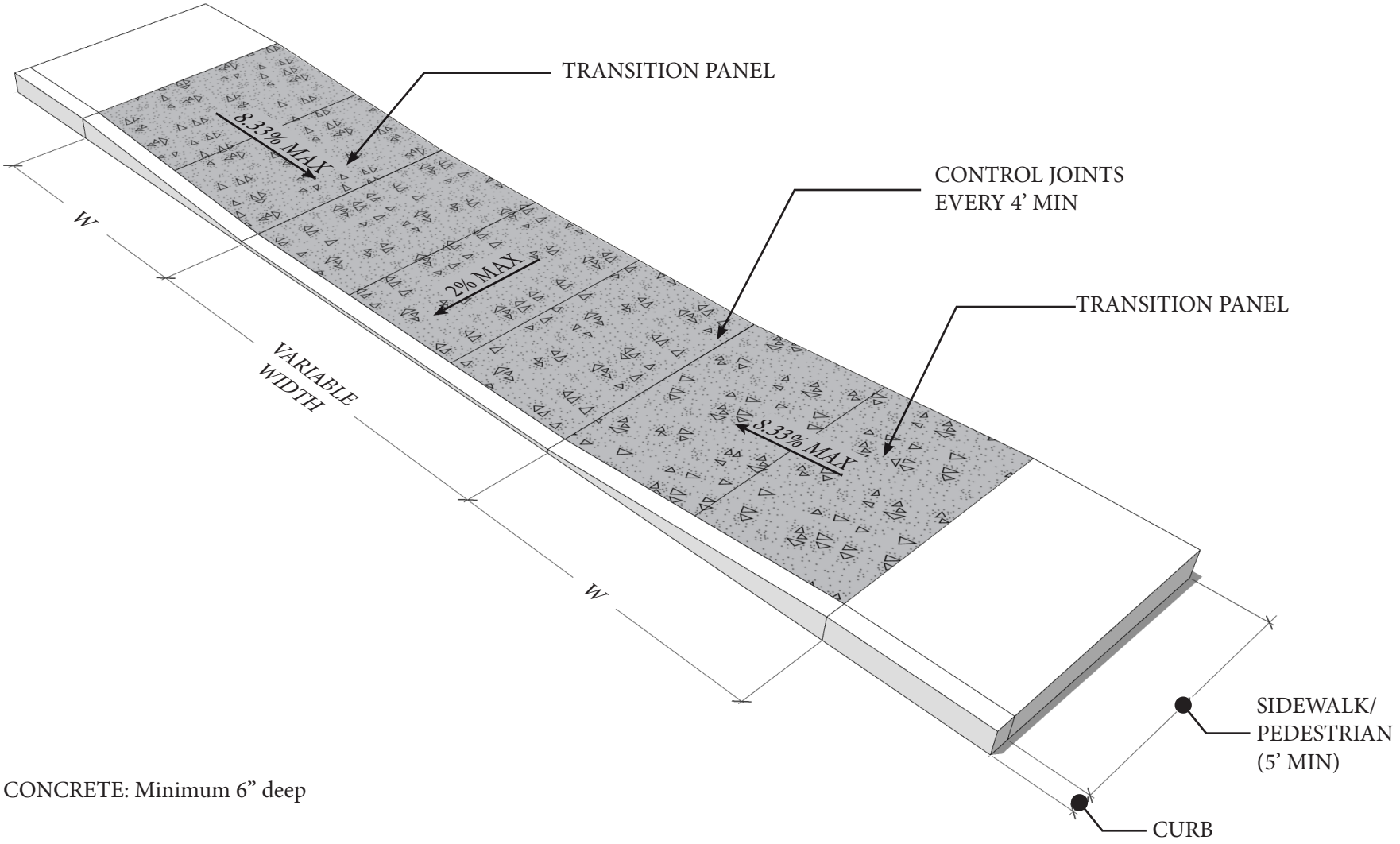






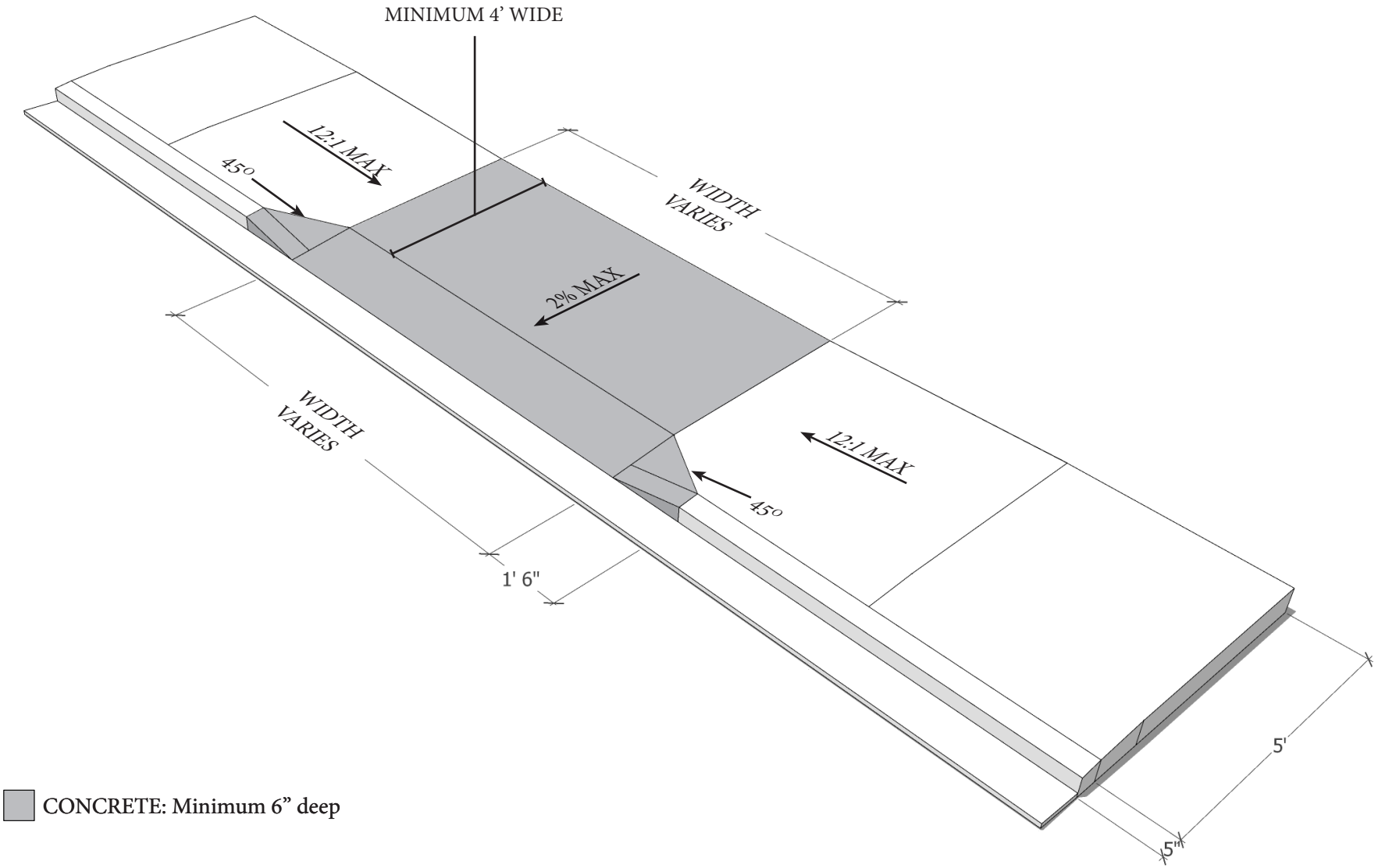
NOTE:

1. Sidewalk and driveways shall have 6 x 6 steel mesh or rebar spaced 6 inches apart.
2. Concrete shall be used for sidewalks and drive approaches and have a compressive strength of not less than 3,5000 P.S.I
3. All edges and joints of the sidewalk and drive shall be rounded. The Surface shall be brushed to create a slightly rough texture



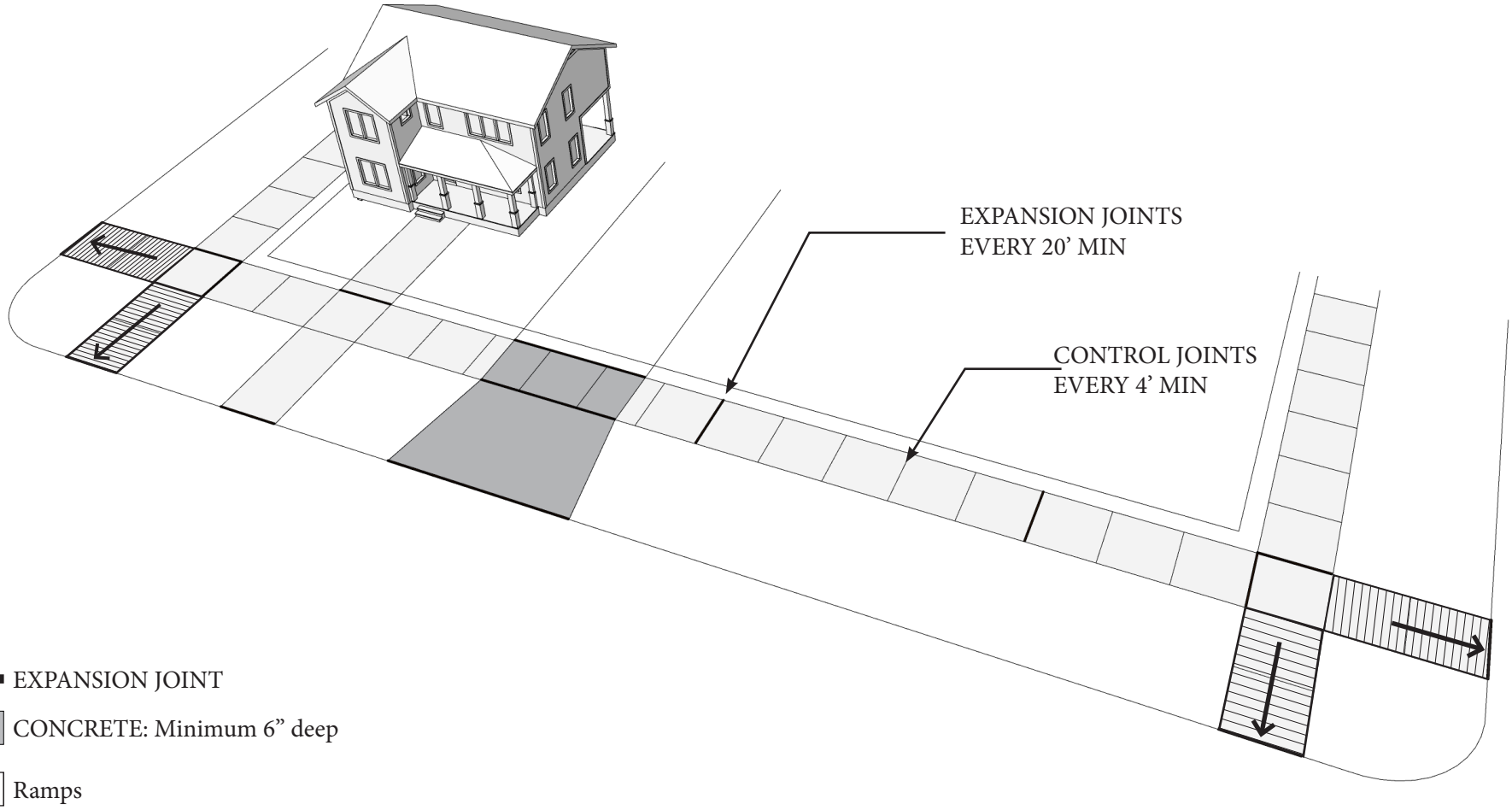
NOTE:

1. Sidewalk and driveways shall have 6 x 6 steel mesh or rebar spaced 6 inches apart.
2. Concrete shall be used for sidewalks and drive approaches and have a compressive strength of not less than 3,5000 P.S.I
3. All edges and joints of the sidewalk and drive shall be rounded. The Surface shall be brushed to create a slightly rough texture



NOTE:

1. Sidewalk and driveways shall have 6 x 6 steel mesh or rebar spaced 6 inches apart.
2. Concrete shall be used for sidewalks and drive approaches and have a compressive strength of not less than 3,5000 P.S.I
3. All edges and joints of the sidewalk and drive shall be rounded. The Surface shall be brushed to create a slightly rough texture



EXPANSION JOINT

CONCRETE: Minimum 6" deep

Ramps

NOTE:

1. Other than areas marked dark grey, all location areas are to be 4" thickness of concrete.
2. Slope on ramps to street a maximum of 8.3%.
3. Truncated domes required at the end of ramps by street

CITY OF CHARLES TOWN
WALKABILITY IMPROVEMENT PROGRAM







City of Charles Town
101 East Washington Street Charles Town, WV 25414

Phone: 304-725-2311
www.charlestownwv.us

Investing in the Future of Charles Town

Charles Town's Walkability Improvement Program is an effort to improve and enhance the overall pedestrian experience in Charles Town. The program is intended to assist applicants in improving the quality of the sidewalks along their property. Improved sidewalks provide safe access to all residents and promote walkability. These benefits contribute to the goals within the City's Comprehensive Plan to improve the pedestrian experience and overall quality of life.

Approved applicants in this program are eligible to receive financial assistance of **50/50 matching funds** for sidewalk repairs or installation, of **up to $7,000; corner lots are eligible for up to $14,000.** The program is managed by the Zoning Administrator. The program components may be amended periodically to accommodate new or modified City policies and procedures.

Policy for Two Bids:

1. **Two Bids** will be required for any application submission.
2. If the work is to be completed by the property owner, verification of expenses is required; only the cost of materials, not labor, is covered for projects completed by the owner.

Policy for Walkability Improvement Program Expiration Date:

1. After an award of a Walkability Improvement Program Grant, the awardee will have one year from the time of the award to complete the improvements.

PROGRAM ELIGIBILITY

All sidewalks in the City of Charles Town are eligible for the grant. Highest priority is for properties with sidewalk gaps. Sidewalks that are in poorest condition will be given high priority. Existing buildings without sidewalks are also eligible. The below matrix from the Charles Town Walkability and Connectivity Study will be used to identify sidewalks that need the most improvement. For an application in which the sidewalks are not identified in the study, the evaluation of the application will be by the same standards by which the study was created:

Priority	Width Assessment	Condition Assessment
1	Poor	Poor
2	Fair	Poor
3	Poor	Fair
4	Good	Poor
5	Poor	Good
6	Fair	Fair
7	Good	Fair
8	Fair	Good
9	Good	Good

INELIGIBLE PROJECTS

New construction projects, government properties, and national franchise properties are not eligible to participate in the Walkability Improvement Program. Private walks extending from the street curb to the main sidewalk, and private service walks extending from the main sidewalks to the home or business, are not eligible.

Ineligible projects may be considered for approval at the discretion of City Council at their first meeting in June, provided no eligible project applications have been received by close of business on the first working day of June.

SIDEWALK MATERIAL

The only permissible materials approved for the Walkability Improvement Program are brick or concrete.

SIDEWALK WIDTH

All sidewalks shall be a minimum of five feet wide, unless constraints on the property do not permit this width. City staff will examine each request and make a determination regarding the ability to install a five foot wide sidewalk.

SURVEY

Where sidewalks do not exist, a survey will be required to ensure that sidewalks are located along the edge of the right-of-way. The cost of the survey as part of the scope of work is eligible for reimbursement.

APPLICATION PROCESS

Each applicant will be eligible to apply up to $7,000.00 ($14,000 for corner lots) each fiscal year. The applicant shall complete and submit the Walkability Improvement Program Application to include the following:

- Proposal, estimates, sketches/photographs, and a written description of the project to be considered for the matching grant;
- Applicants must provide the 50% matching portion of the estimated project cost and submit proposed/estimated cost in the application. A **minimum of two bids** must be provided; and
- Grant Approval Agreement will be signed by the property owner.

CONDITIONS OF APPROVAL

In addition to previously listed requirements, all properties must be paid to date on all municipal taxes. Each property will be eligible for one grant per twelve (12) month period. The Zoning Administrator may add conditions of approval of the Grant application, as necessary.

APPROVAL PROCEDURES

Each application will be reviewed, and the property will be deemed eligible or ineligible for grant funding, by the Zoning Administrator. If deemed eligible, staff will make a decision based on compliance of the project with the Charles Town Walkability and Connectivity Study and the Ordinances of the City of Charles Town. If the application is denied, the applicant will receive notification and an explanation of the denial. Staff may provide recommendations for modifications that could be made for the project to receive consideration for approval.

APPROVED PROJECT

The City will contact the applicant and the following shall occur:

- apply for and obtain all necessary permits.
- submit receipts/invoices to the City once the project is complete for reimbursement.

Construction may begin only after the application has been approved. Any work completed prior to formal written approval will not be eligible for the match funding.

PROJECT MANAGEMENT

All applicants accepted into the Walkability Improvement Program will be fully responsible for managing construction of projects, including, but not limited to: obtaining bids, selecting contractors, obtaining approvals, permits, and insurance, overseeing construction work, and paying all invoices for work, materials, and supplies. Any contractor or subcontractor must have a valid business license issued by the City of Charles Town. The applicant is responsible for ensuring that all contractors and subcontractors meet these requirements. Any contractor or subcontractor working on the project must be licensed and insured.

Applicants shall solicit bids and proposals, materials, and labor from qualified local residents and businesses whenever possible.

NON-DISCRIMINATION - EQUAL EMPLOYMENT OPPORTUNTY

Applicants shall follow the City's non-discrimination ordinance and equal employment opportunity requirements in the solicitation of contractors, subcontractors, workers, and suppliers.

CITY ACCOUNTABILITY

The City's participation in this program does not make the city liable regarding the quality and/or soundness of construction, repairs, additions, or removals.

PAYMENT OF MATCHING FUNDS

Upon completion of the project, the Applicant will provide accounting of all project costs and a copy of all paid invoices. Projects must be completed within twelve (12) months after formal approval has been granted. Any time extension request must be filed with and approved by the Zoning Administrator.

Reimbursement will be issued after the property owner's portion of the project has been completed (including site inspections), and the City has received receipts detailing the completed work. If the project meets all standards, the City will provide funding for no more than the amount awarded in the grant application.

APPLYING AS A TENANT

The property owner of record's signature shall be required on all applications, and no application will be accepted if the property owner's signature is not present.

APPLYING AS A BUSINESS

Any business applying for these grant funds must provide a copy of their business license.

ADDITIONAL INFORMATION

The City recommends that any applicant(s) interested in applying for acceptance into the Walkability Improvement Program contact the Zoning Administrator prior to submitting an application. Applications may be obtained at City Hall and at www.charlestownwv.us.

CITY OF CHARLES TOWN
WALKABILITY IMPROVEMENT PROGRAM

Applicant's Name: _____

Application Submission Date: _____

Phone: _____

E-mail: _____

Mailing Address:_____

_____

The name of the person/entity the reimbursement check is to be made out to, and their mailing address, if different from the information provided above:

_____

_____

Project Address:

_____

Has the property in this application been awarded a Sidewalk Improvement Program grant in the past 12 months?

☐ Yes ☐ No

Projects that answer yes to any of the following questions are **not eligible** for the program:

Is this property:

New Construction?	Yes ___	No ___
A Government-owned property?	Yes ___	No ___
A national franchise?	Yes ___	No ___

Description of the Walkability Improvement project:

_____

_____

Estimated Project Start Date: _____

Estimated Project Completion Date: _____

Estimated Total Project Cost: $_____

Grant Amount Requested: $_____

I have reviewed the following documents:

- ☐ Codified Ordinances of the City of Charles Town
- ☐ Construction Details for Sidewalks

Upon approval of the application the following will be required by the applicant:

- Obtain all necessary building permits;
- Pass required City inspections;
- Submit receipts/invoices to the City upon completion of the project;

CERTIFICATION

- I agree to follow the plan submitted with the application and I understand that failure to do so may disqualify the project for grant funding;
- I swear and affirm that I shall not discriminate in solicitation of contractor, subcontractors, workers, or suppliers.
- I agree to complete all improvements within one year of approval from the approval of the grant. Any time extension must be filed and approved by the Zoning Administrator;
- I agree and understand that I have to provide receipts related to the project. If a contractor was used, a written invoice must be provided to the City and receipts and invoices must be accompanied by proof of payment (i.e. cancelled checks), before funds will be granted. If a contractor was not used, receipts must be provided to the City Staff before a reimbursement will be issued. Only materials may be reimbursed for projects that do not use a contractor.
- I agree and understand that grant monies shall not be distributed until all proposed work is completed and has passed inspected.
- I agree that the information provided above and within this application is accurate and correct to the best of my knowledge. I also assure that the property listed is in compliance with all laws, ordinances, rules, and regulations of the State of West Virginia and the City of Charles Town.

Signatures are required on the next page

Property Owner's **Signature:** _____

Date: _____

Applicant's **Signature:** _____

Date: _____

Please submit an original completed petition to the following:

Zoning Administrator

City of Charles Town

101 E. Washington Street Charles Town, WV 25414

FOR CITY USE ONLY

Application Number:_____ Date Application Received:_____

Zoning District: _____

Business license provided (Yes/Not Applicable) _____

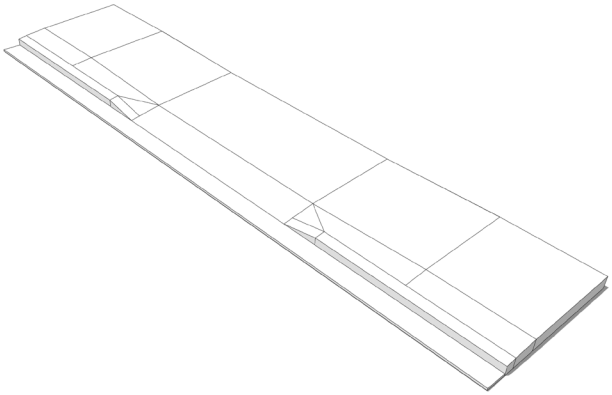
Receipt No._____ Approval/Denial:_____ Decision Date:_____

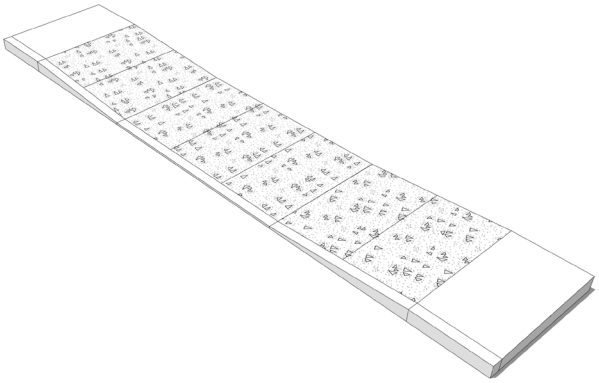
Comments:_____

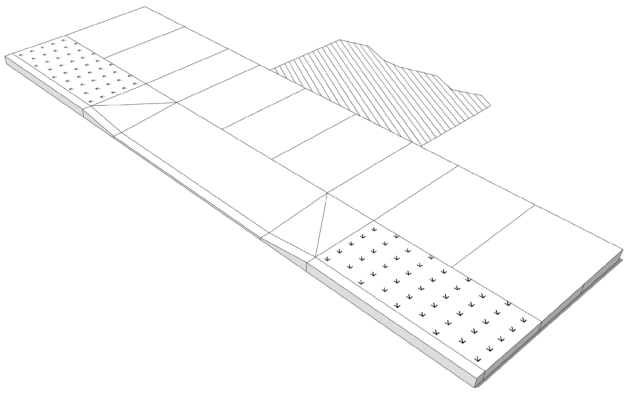
_____

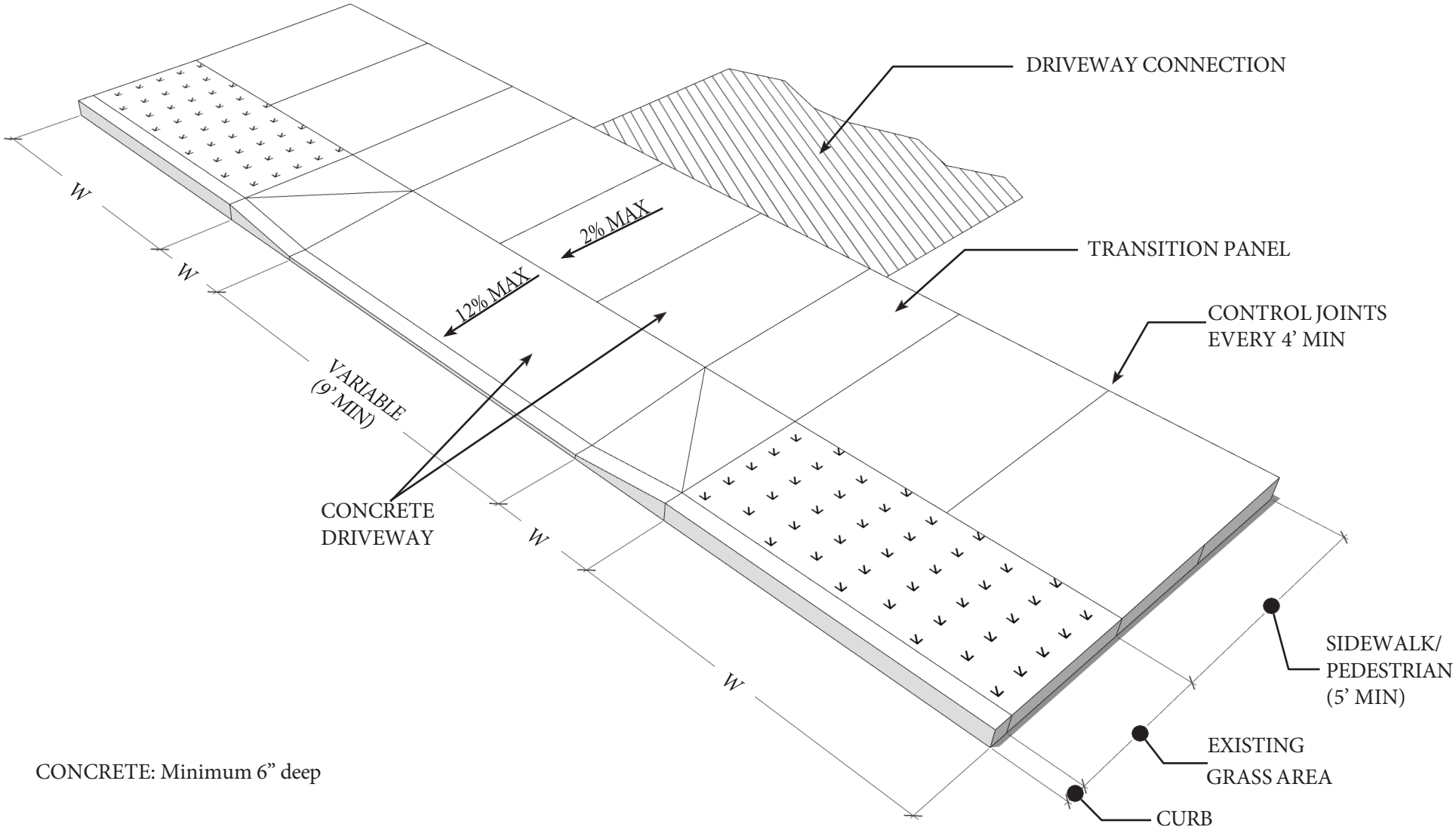
Staff Signature:

SIDEWALK
IMPROVEMENT
STANDARD DETAILS



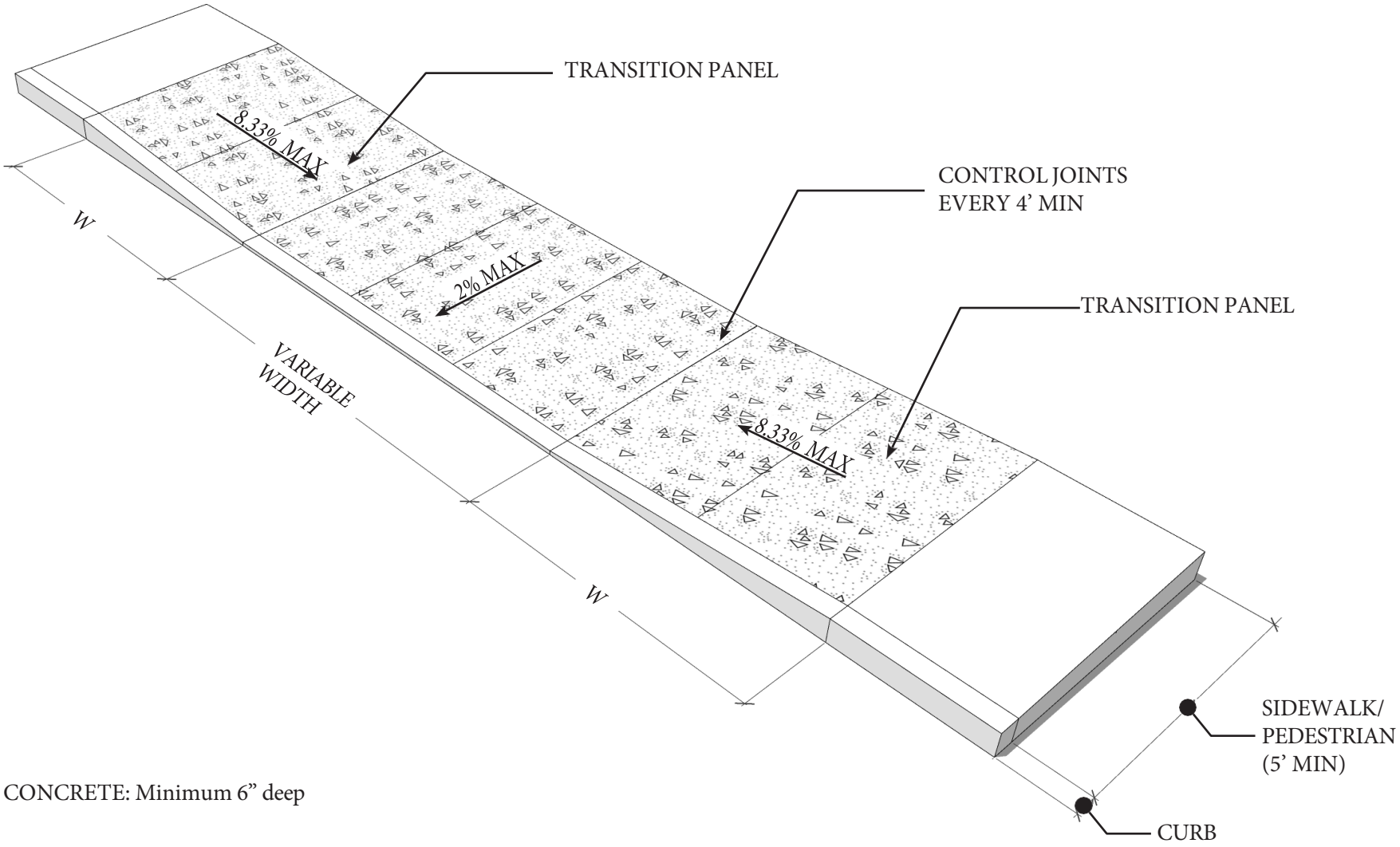




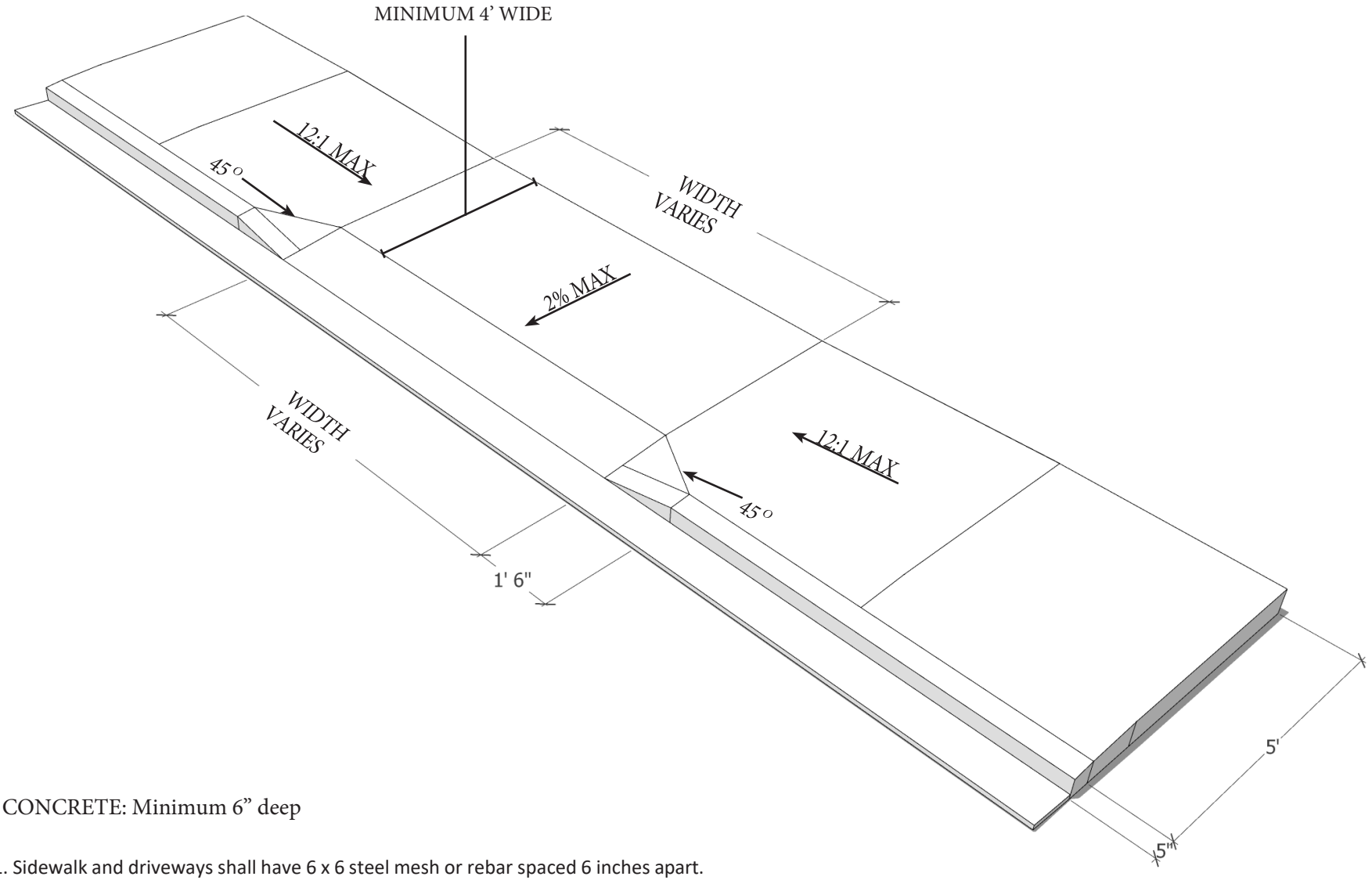


CONCRETE: Minimum 6" deep

1. Sidewalk and driveways shall have 6 x 6 steel mesh or rebar spaced 6 inches apart.
2. Concrete shall be used for sidewalks and drive approaches and have a compressive strength of not less than 3,500 P.S.I
3. All edges and joints of the sidewalk and drive shall be rounded. The Surface shall be brushed to create a slightly rough texture

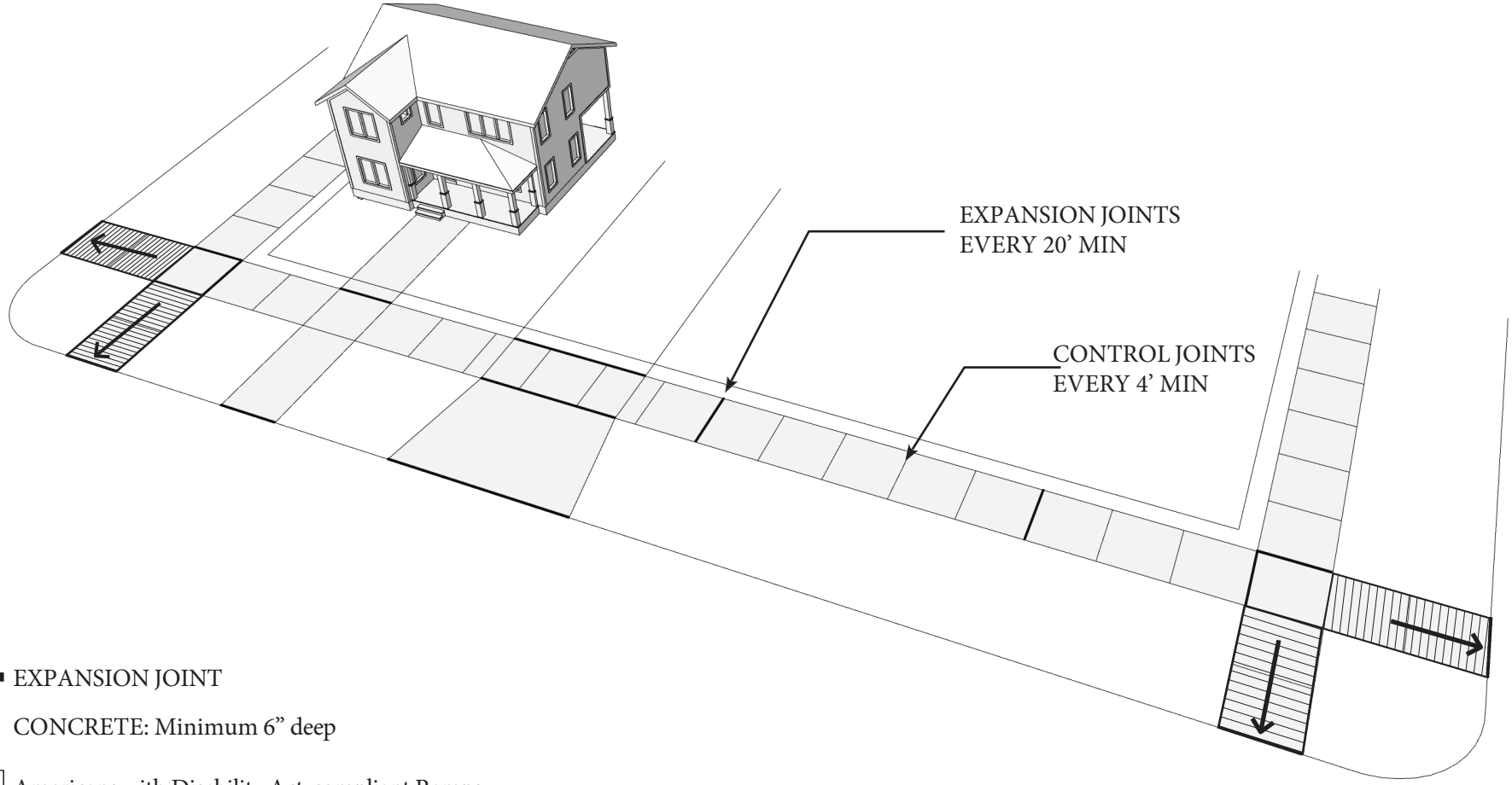


1. Sidewalk and driveways shall have 6 x 6 steel mesh or rebar spaced 6 inches apart.
2. Concrete shall be used for sidewalks and drive approaches and have a compressive strength of not less than 3,500 P.S.I
3. All edges and joints of the sidewalk and drive shall be rounded. The Surface shall be brushed to create a slightly rough texture



CONCRETE: Minimum 6" deep

1. Sidewalk and driveways shall have 6 x 6 steel mesh or rebar spaced 6 inches apart.
2. Concrete shall be used for sidewalks and drive approaches and have a compressive strength of not less than 3,500 P.S.I
3. All edges and joints of the sidewalk and drive shall be rounded. The Surface shall be brushed to create a slightly rough texture



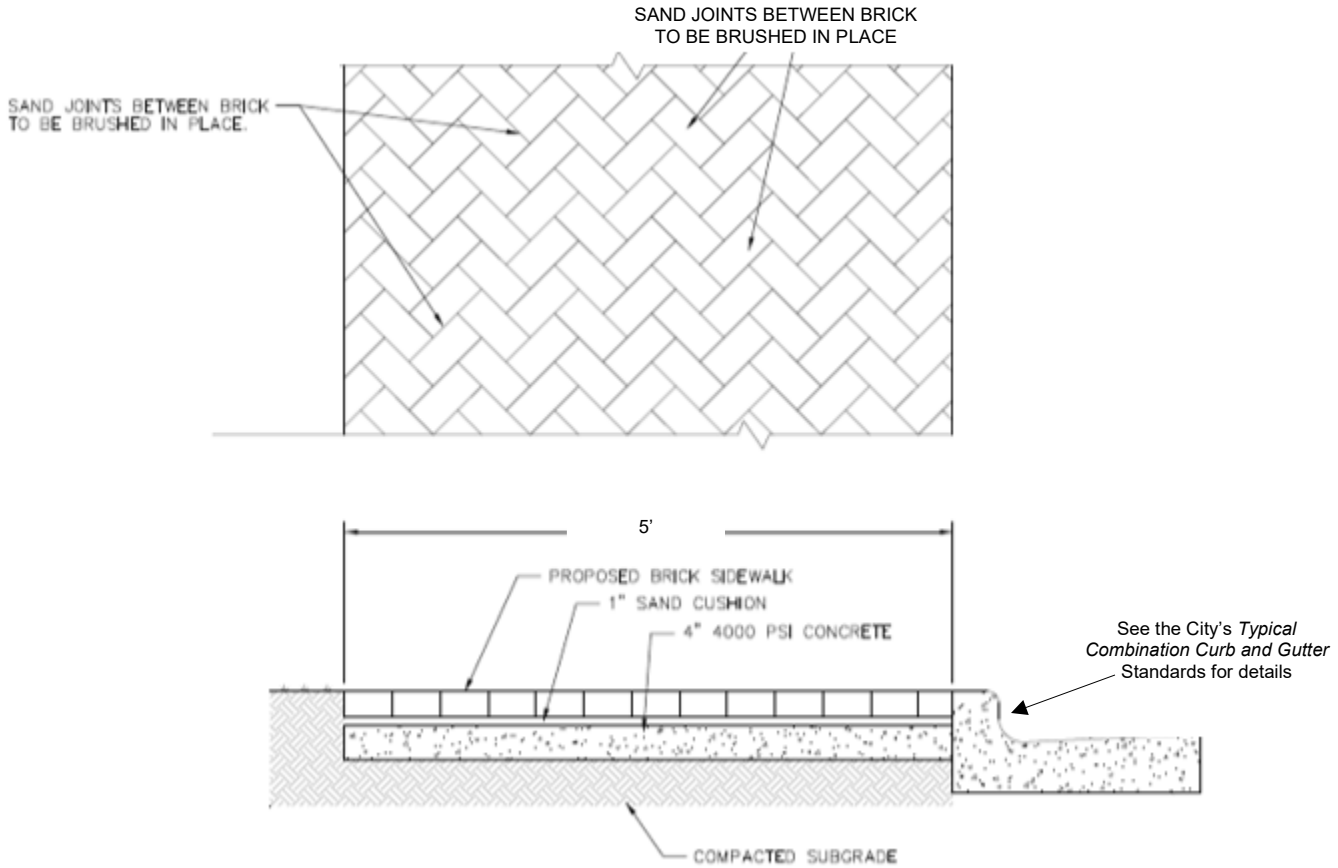
EXPANSION JOINT

CONCRETE: Minimum 6" deep

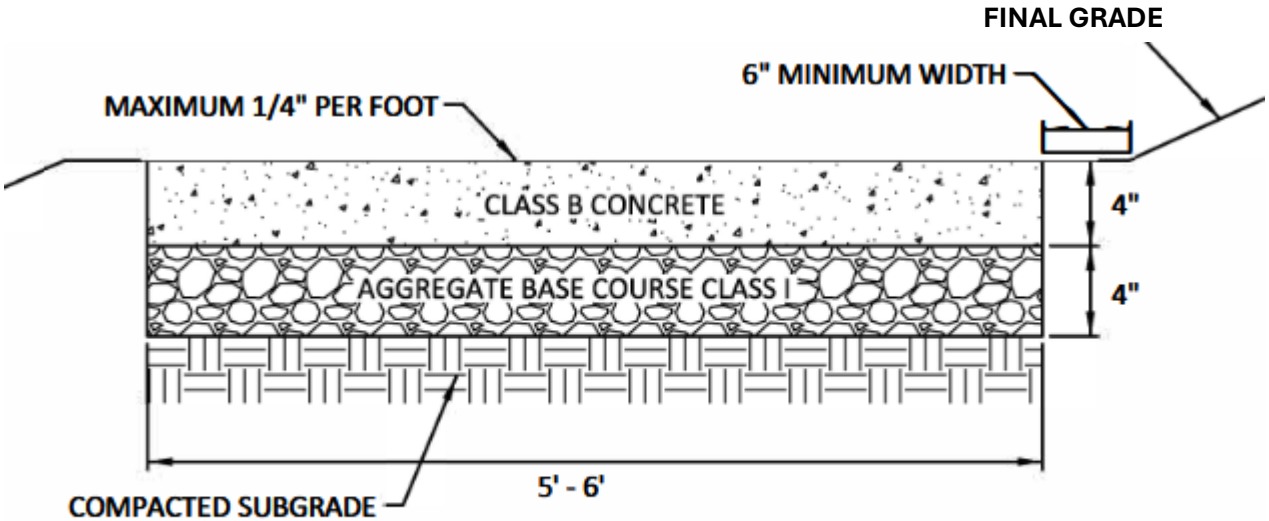
Americans with Disability Act-compliant Ramps

1. Other than areas marked dark grey, all location areas are to be 4" thickness of concrete.
2. Slope on ramps to street a maximum of 8.3%.
3. Truncated domes required at the end of ramps by street

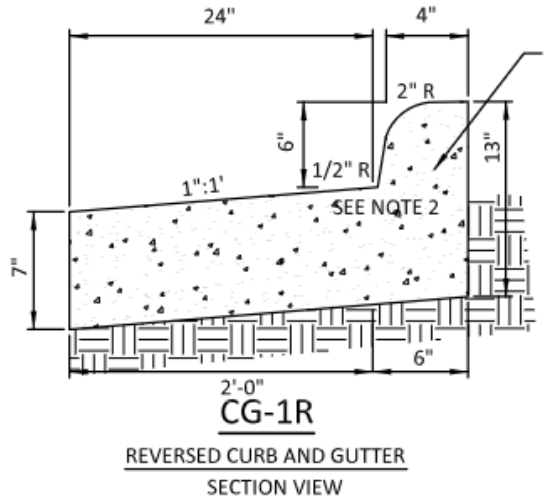
Brick Sidewalk Design Standards:
No specific pattern is required.



Concrete Sidewalk Design Standards:



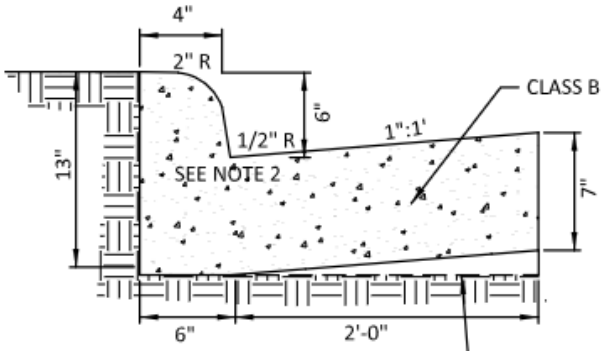
STANDARD SIDEWALK (SW-1)



CG-1R

REVERSED CURB AND GUTTER

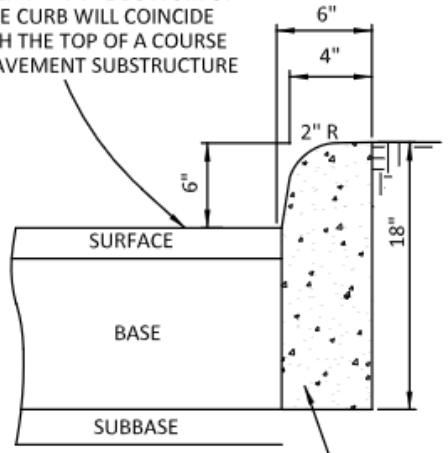
SECTION VIEW



CG-1

STANDARD CURB AND GUTTER

THE DEPTH OF CURB MAY BE REDUCED AS MUCH AS THREE INCHES OR INCREASED AS MUCH AS THREE INCHES IN ORDER THAT THE BOTTOM OF THE CURB WILL COINCIDE WITH THE TOP OF A COURSE OF PAVEMENT SUBSTRUCTURE



CG-2

MEDIAN CURB

THE BOTTOM OF THE CURB AND GUTTER MAY BE CONSTRUCTED PARALLEL TO THE SLOPE OF THE SUBSURFACE COURSES PROVIDED A MINIMUM OF 7" IS MAINTAINED.

NOTES:

1. THE USE OF CG-1R SHALL NOT BE UTILIZED WITHIN THE LIMITS OF PUBLIC RIGHT OF WAY.
2. A MAXIMUM OF A 2" RADIUS IS ACCEPTABLE WITH CURB AND GUTTER.
3. SUBGRADE FOR ALL CURB AND GUTTER SHALL BE COMPACTED TO 95 PERCENT DENSITY AT OPTIMUM MOISTURE TO THE FULL WIDTH OF RIGHT OF WAY IN ACCORDANCE WITH AASHTO, T99.

NOT TO SCALE

TYPICAL COMBINATION CURB AND GUTTER

City of Charles Town

CG-1
CG-1R
CG-2

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

Facade Improvement Grant - Updates

ATTACHMENTS:

- 1. Staff Report.pdf
- 2. FIP Application- CURRENT.pdf
- 3. FIP Application- DRAFT Version with changes.pdf

Date: For the October 19, 2026 City Council meeting
From: James Newman, City Planner, Zoning/Subdivision Administrator

Facade Improvement Grant – Proposed Changes

1. **Facade Improvement Grant – Current Parameters**
   This grant is currently reviewed and approved or denied by the Historic Landmarks Commission The purpose of the grant is to aid in "*beautifying and rehabilitating property fronts for the purposes of attracting both customers and prospective business owners, and serving as a tool for revitalization of the downtown area.*"

   The Grant acts a Certificate of Appropriateness, so currently requires legal notice an d a posted sign, as well as a public hearing before the Commission.

2. **City Council**
   At their meeting on October 5, 2026, City Council discussed changes to the Grant program following a recent appeal of a Grant denial by the Commission. Council discussion included making the grant subject to administrative review rather than review by the Commission, changing the Grant amount to account for inflation, and removing sign installation from the list of permitted uses for Grant funds.

3. **Changes in the Draft Version**
   A. Increase the payment cap from $5,000 to $7,000 to keep up with inflation.

   B. Removed the reference to 'sign removal, installation, or repair' from the list of Eligible Projects. Only 'Sign Repair' remains eligible.

   C. Specifically added 'installation of new signage' to the list of Ineligible Projects.

   D. Moved Grant approval and denial from the Historic Landmarks Commission to the Zoning Administrator, and removed the requirement for public notice.

   E. General reformatting.

4. **Certificate of Appropriateness**
   A Certificate of Appropriateness is still required for work which meets the threshold for requiring a Certificate. The Certificate must be approved prior to obtaining Grant approval.

F. Recommendation
Approval of the proposed changes.

CITY OF CHARLES TOWN

Department Community Development
Division of Planning & Zoning

101 East Washington Street, P.O. Box 14, Charles Town, WV 25414
Phone: (304) 724-3248 ♦ Fax: (304) 725-1014 ♦ Web: www.charlestownwv.us

To: Applicants of the Façade Improvement Program
From: Seth A. Rivard, Director of Community Development
Date: October 15, 2018
Subject: Façade Improvement Program Submission Requirements

Policy for Façade Improvement Program for paint and materials:

1. Appropriate paint colors for Charles Town are color tones that would have been traditionally and predominately found in the mid-Atlantic region. Colors on a structure must be appropriate to the period from which the structure was constructed. (this applies to FIP and would be a general statement of recommendation that identify the types of the colors the Design Review Standards states "must" be used).
2. Color tones chosen should complement the details of the building and the composition of the color should not obscure or hide the details.
3. For depiction purposes, six (6) samples of the paint swatches will be required to be submitted. This will allow one sample of chosen paint colors per HLC member and one for the file. Renderings are allowed, but are not a substitution of the paint swatches.
4. In the event the applicant changes material or paint colors once an application is submitted, the applicant shall provide updated material to the Department of Community Development.

Policy for Two Bids:

1. **Two Bids** will be required for any application submission.
2. If the work is to be completed by the property owner, verification of expenses by a bid or a site such as homewyse.com will be required.

Policy on Composite Material:

1. The HLC, at its discretion, may consider composite material. The HLC will closely examine how the composite material will look in relationship to the original material. This could include, but is not limited to, shape, size, profile and texture. At least one sample of the proposed material will be required at time of application submission.

Policy for Façade Improvement Program Expiration Date:

1. After an award of a Façade Improvement Program Grant, the awardee will have one year from the time of the award to complete the improvements.

Yard Sign

1. “This project was funded in part through the City of Charles Town’s Façade Improvement Program.” This sign shall be posted for a minimum of 3 weeks and should be up while the project activity is underway.

CITY OF CHARLES TOWN
FAÇADE IMPROVEMENT PROGRAM







City of Charles Town
101 East Washington Street
Charles Town, WV 25414

Phone: 304-724-3248
Fax: 304-725-1014
Website: www.charlestownwv.us

Investing in the Future of Charles Town

Charles Town's Façade Improvement Program was designed as an effort to improve and enhance the overall look and experience of downtown Charles Town. The program is intended to assist property owners and/or tenants within the Charles Town Historic Overlay District (HOD) in beautifying and rehabilitating property fronts for the purposes of attracting both customers and prospective business owners and serving as a tool for revitalization of the downtown area.

Property owners or tenants who choose to participate in this program are eligible to receive financial assistance, in the form of a **50/50 funds match, up to $5,000.00**, for eligible projects and revitalization efforts in the Historic Overlay District of Charles Town. The program is managed by the City of Charles Town's Historic Landmarks Commission. Design and program components may be amended periodically to accommodate new or modified City policies and procedures.

PROGRAM ELIGIBILITY

Property owners who own properties within the boundaries of the Historic Overlay District, or their tenants, are eligible to apply for the program.

ELIGIBLE PROJECTS

All projects accepted for the program must reflect "true to age" improvements. All improvements must be consistent with Design Review Standards established by the Charles Town Historic Landmarks Commission (CTHLC) as well as the Codified Ordinances of the City of Charles Town. Only exterior, street-facing improvements are eligible to receive match funding. Eligible improvements include, but are not limited to:

- Awnings appropriate for the façade improvement and architecture;
- Exterior painting consistent with other downtown buildings and accepted as recognized historical coloring;
- Non-illuminating signs that are compatible with other buildings on the block and that conform to Historic Landmarks Commission Standards and the Codified Ordinances of the City of Charles Town;
- Exterior masonry repair;
- Repair to exterior facades that face the street or corners in which one side faces the street;
- Sign removal, replacement, or repair that follows Historic Landmarks Commission Standards and the Codified Ordinances of the City of Charles Town;
- Repair or replacement to cornices, windows, decorative detail, doors, awnings, or window display lighting;
- Exterior lighting structures and hardware on the street-facing side of the building;
- Structural landscaping features;

- Addition or modification to entryways that allow for greater access for people with disabilities;
- Reconstruction of features that were part of the original structure and can be documented;
- Removal of historically inappropriate elements or features.

INELIGIBLE PROJECTS

New construction projects, government properties, and national franchise properties are not eligible to participate in the Façade Improvement Program. Ineligible improvements include:

- Interior improvements;
- Roofing;
- Paving;
- Structural improvements;
- Security measures;
- Loading docks;
- Parking entrances;
- Removal of structurally important features.

APPLICATION PROCESS

Each applicant will be eligible to apply for up to $5,000.00 each fiscal year. In order to be considered for a Façade Improvement Program 50/50 matching grant, the property owner and tenant shall complete the following tasks:

1. Review the Design Review Standards, including eligible and ineligible projects.
2. Complete and submit the Certificate of Appropriateness Application and Façade Improvement Program Application.
3. Submit before and after sketches, photographs, or other illustrations and a written, detailed description of the project to be considered for the matching grant.
4. Complete the property owner's or tenant's 50% matching portion of the estimated project cost and submit proposed/estimated cost. Bids must be provided if the work is being done by a contractor.

If the application and request is approved, the following will be required:

5. Apply for and obtain all necessary permits.
6. Submit receipts/invoices to the City once the project is complete.

CONDITIONS OF APPROVAL

Proposals, estimates, sketches/photographs, and project descriptions will be reviewed by the CTHLC and a determination will be made as to acceptance into the program. In addition to previously listed requirements, all properties must be paid to date on all municipal taxes. Each property will be eligible for one grant per twelve (12) month period. Grants may be limited based on availability.

APPROVAL PROCEDURES

Upon receipt of application and required materials for consideration, each application will be reviewed and the property will be deemed eligible or ineligible for grant funding by staff. If deemed eligible, The HLC will make a decision based on compliance of the project with the Charles Town Historic Landmarks Commission Design Review Standards, the Codified Ordinances of the City of Charles Town, and character of the project as compared with existing properties in the surrounding area. **Since the awarding of the grant funding will also act as approval of the Certificate of Appropriateness (COA), *both* the COA application and Façade Improvement Program Application will need to be submitted together for review and consideration.**

If approved for grant funding, the City will contact the applicant, a Grant Approval Agreement will be signed by the property owner, and the applicant may begin his/her matching portion of the project. If the application is denied, the applicant will receive notification and an explanation of the denial. The City may also provide recommendations for modifications that could be made in order for the project to receive consideration for approval at a later date.

PROJECT MANAGEMENT

All property owners or tenants accepted into the Façade Improvement Program will be fully responsible for managing construction of projects, including, but not limited to, obtaining bids, selecting contractors, obtaining approvals, permits, and insurance, overseeing construction work, and paying all invoices for work, materials, and supplies.

The City of Charles Town encourages employment and business opportunities for local residents and businesses. Participants shall seek to solicit bids and proposals, materials, and labor from qualified local residents and businesses whenever possible.

Property owners or tenants may not discriminate on the basis of race, gender, religion, national origin, ethnicity, ancestry, origin, sexual orientation, marital status, creed, age, or disability in the solicitation of contractors, subcontractors, workers, and suppliers.

The City makes no guarantees on quality and soundness of construction or other repairs, additions, or removals. Any contractor or subcontractor working on the project must be licensed and insured. In addition, any contractor or subcontractor must have a valid business license issued by the City of Charles Town. The property owner or tenant is responsible for ensuring that all contractors and subcontractors meet these requirements.

PAYMENT OF MATCHING FUNDS

Construction may begin only after the application has been approved by the Historic Landmarks Commission, an agreement has been signed, all required permits have been obtained, and formal approval to begin the project has been given to the applicant in writing. **Any work completed prior to formal written approval will not be eligible for funding.**

Grants will be issued after the property owner's portion of the project has been completed and the City has received receipts detailing the completed work. Upon completion, City staff must be contacted for a site inspection. If the project meets all standards, the City shall provide funding for no more than 50% of the total cost of the project, not to exceed $5,000.00.

Upon completion of the project, the Applicant will provide accounting of all project costs and a copy of all paid invoices. Projects must be completed within twelve (12) months after formal approval has been granted.

APPLYING AS A TENANT

Tenants applying for the Façade Improvement Program shall have the property owner's permission to make any improvements detailed in the COA. The property owner of record signature shall be required on all applications and no application will be accepted if the property owner signature is not present.

ADDITIONAL INFORMATION

The City recommends that any property owner or tenants interested in applying for acceptance into the Façade Improvement Program contact City staff prior to submitting an application. Questions about the program may be directed to the City Planner. Applications may be obtained at City Hall and at www.charlestownwv.us.

APPLICATION

Applicant's Name: _____ Date: ____/____/____
Day Month Year

Company Name: _____ Phone: _____

Mailing Address: _____ Fax: _____

_____ E-mail: _____

Project Address: _____ , Charles Town, WV 25414

Have you received rebates from the City's Façade Improvement Program in the past 12 months? ☐Yes ☐No

Is this property:

New construction? ☐Yes ☐No

Government-owned property? ☐Yes ☐No

A national franchise? ☐Yes ☐No

Description of the Façade Improvement project:

_____

_____

_____

_____

_____

_____

Estimated Project Start Date: ____/____/____ (Day / Month / Year)
Estimated Project End Date: ____/____/____ (Day / Month / Year)

Estimated Total Project Budget: _____

Grant Amount Requested: _____

The following items are included with this application:

- ❑ Before/after sketches or photographs or illustrations
- ❑ Detailed proposal and/or contractor estimates

I have reviewed the following documents, as they pertain to my application:

- ❑ Codified Ordinances of the City of Charles Town
- ❑ Charles Town Historic Landmarks Commission Design Review Standards
- ❑ Façade Improvement Program Manual

<u>If the application and request is approved, the following will be required</u>:

- Apply for and obtain all necessary permits.
- Submit receipts/invoices to the City once the project is complete.
- City inspection of improvements to ensure compliance with the COA and intended outcomes based on the funding application submittal.

I agree that the information provided above and within is accurate and correct to the best of my knowledge. I also assure that the property listed is in compliance with all laws, ordinances, rules, and regulations of the State of West Virginia and the City of Charles Town.

Property Owner's Printed Name: _____

Property Owner's Signature: _____

Date of Application: _____

Tenant's Signature: _____
(If tenant is undertaking the proposed work)

COA Application No._____

CERTIFICATE OF APPROPRIATENESS APPLICATION

ZONING ORDINANCE SECTION 1322.13, HISTORIC OVERLAY DISTRICT
AND
ARTICLE 141 OF THE CHARLES TOWN CODIFIED ORDINANCE
AND
DESIGN REVIEW STANDARDS

All proposed activity must be approved by the Historic Landmarks Commission (HLC) via issuance of a Certificate of Appropriateness (COA).

Many of the activities for which a COA is required also requires building permit, which is a separate process from obtaining a COA.

If applying for the Façade Improvement Program, the "Addendum – Façade Improvement Program" will be required in addition to this application.

1. APPLICANT'S NAME _____

Address: _____

Telephone Number: (___) _____ Fax Number (___) _____

Email Address: _____

Relationship to Owner: ___Lessee ___Contractor ___Architect ___Consultant ____Other: (explain)_____

2. CURRENT PROPERTY OWNER'S NAME_____

Address: _____

Telephone Number: (___) _____ Fax Number (___) _____

Email Address: _____

3. PHYSICAL ADDRESS: _____

Tax Map # and Parcel(s): _____

Zoning District: _____

4. DESCRIPTION OF FORMER USE(S) OF THE PROPERTY

_____

_____

5. DESCRIBE THE CURRENT OR PROPOSED USE OF THE SUBJECT PROPERTY

_____

_____

_____

_____

6. TYPE OF WORK:

A. _____ Exterior alteration or repairs.

B. _____ New Construction: 1)____Primary Structure; 2)____Garage;
3)____New Addition; 4)____Other;

C. _____Demolition: 1)____Whole Structure; 2)____Part of Structure;

D. _____Relocation of Structure

7. EXTERIOR ALTERATION OR REPAIR

A. Check all that apply for which approval of the proposed activity is requested.

____Architectural feature (decorative ornamentation)	____Metal trim	____Iron fences
____Material changes (wood, brick, metal, etc.)	____Windows - replacement, removal, elimination or new opening	____New construction
____Roof – Change in shape/profile	____Shutters	____Additions or alterations
____Skylights or dormers	____Door and transoms	____Signs
____Masonry - cleaning, tuckpointing, removal of masonry or other changes to the masonry	____Cut stone steps	____Solar panels
____Removal of historic markings and paintings	____Security Features	____Mothballing
____Wood cornices and concealed box gutters	____Porch or deck	____Demolition
____Wood trim	____Awnings and canopies	

B. List and describe in detail all work to be done for each item checked. Include the following materials when appropriate:

1) Sketches, photographs, specifications, manufacturer's illustrations or other description of proposed changes to the building's exterior. Detailed drawings are required for major changes in architectural features.
2) If material changes are proposed, please provide a description of them. The architect's specifications or brochures may suffice; however, the Commission may request samples of new materials.

C. SIGNS:

1) See page 6 of this application for more information.
2) Signage activities are regulated under Article 1324 (Signs) and Section 1322.13 (Historic Overlay District) of the City of Charles Town's Zoning Ordinance and by extension the Design Review Standards. **All permitted sign sizes, location of placement and additional sign standards are regulated by Article 1324 and shall meet those standards.** The HLC role is to review the sign for appropriateness within the Historic Overlay District.

D. NEW CONSTRUCTION: Describe the nature of the proposed project. Include the following materials when appropriate:

1) Site plan with measured distances.
2) Elevation drawings of each façade and specifications which clearly show the exterior appearance of the project.
3) Samples or other description of materials to be used.
4) Drawings or other description of site improvements such as fences, sidewalks, lighting, pavement, decks, etc.

E. DEMOLITION OF STRUCTURE

1) Describe the structure's condition and reason for demolition.
2) Additional criteria is found in the Design Review Standards, including the need to prove economic hardship.
3) Describe the proposed reuse of the site, including drawings of any proposed new structure or landscaping.

F. RELOCATION OF STRUCTURE

1) Explain what will be moved, why, and proposed changes.
2) If a building will be moved into a district from outside, include photographs.
3) Include a site plan of the proposed location in the district and describe any site features which will be altered or may be disturbed, including foundations, walls, vegetation, etc.

G. MOTHBALLING OF STRUCTURE

1) Describe how the structure will be secured from unwanted entry.
2) Describe measures to be taken to keep the weather and pest out.
3) If the property owner will not be in the state of West Virginia, designate a local contact.
4) If any door(s) or window(s) are to be boarded up, they must be painted to look like a door or window or decals that look like door and window must be adhered to the boards on the window or door.
5) Additional criteria is found in the Design Review Standards, including the need to prove economic hardship.
6) Describe how the property will be maintained so as to not become a code violation, such yard maintenance.

DESCRIPTION OF THE PROPOSED ACTIVITY:

_____

_____

_____

_____

_____

_____

_____

_____

CERTIFICATION

I certify that, to the best of my knowledge, the submitted information and statements are true and correct. I also certify that I have received and read Article 1324, Section 1322.12, of the Zoning Ordinance and relevant provisions of the Charles Town Design Review Standards pertaining to this application.

Signature of Applicant

_____ Date _____

Signature of Property Owner

_____ Date _____

Please submit an original completed petition to the following:

Zoning Administrator
City of Charles Town
101 E. Washington Street
Charles Town, WV 25414

Signs – Additional Information

ESTIMATED COST OF SIGN(S) (Excluding Labor & Installation):

_____

SIGN CONTRACTOR:

_____

Contractor License #: WV & City of Charles Town:

_____

TYPE OF SIGN

Type of Sign	Check One	Type of Sign	Check One
Free Standing		Suspended	
Building Mounted		Awning	
Window Lettering		Other (List)	

Where on the property or building will the sign(s) be located?

_____

SIGN MATERIAL:

_____

SIGN DIMENSIONS:

Height	Width	Depth

WILL SIGN(S) BE LIGHTED? If yes, list the type of lighting to be used:

_____

PLEASE PROVIDE PROOF OF INSURANCE (In case of sign damage) Insurance Company:

_____

PROVIDE AN ILLUSTRATION OR PHOTOGRAPH OF THE PROPOSED SIGN(S)

FOR CITY USE ONLY

Application Number:_____ Date Application Received:_____

Zoning District: _____

Fee: $_____ Paid: $_____ Check No._____

Receipt No._____

Zoning Administrator Approval:_____ Date:_____

Historic Landmarks Commission Approval:_____Date:_____

Comments:_____

_____

_____

_____

_____

_____

Grant Approval Agreement

1. **I understand that grant monies shall not be distributed until all proposed work is completed and inspected.**

2. **I understand that I have to provide receipts related to the project. If a contractor was used, a written invoice must be provided to the City before funds will be granted. For projects that involve a contractor, receipts and invoices must be accompanied by proof of payment (i.e. cancelled checks). If a contractor was not used, receipts must be provided to the City Staff before a reimbursement will be issued. Only materials may be reimbursed for projects that do not use a contractor. Receipts and invoices must be accompanied by proof of payment (i.e. cancelled checks).**

3. **I understand that an inspection of the project must be performed by City staff upon completion of the project.**

4. **I agree to follow the plan submitted with the application and I understand that failure to do so may disqualify the project for grant funding.**

5. **I agree to all of the attached "Conditions of Approval", if any, as developed by the Historic Landmarks Commission.**

6. **I agree to complete all improvements within one year of approval from the Historic Landmarks Commission. Any time extension must be filed and approved by the Historic Landmarks Commission.**

Property Owners Signature _____ **Date** _____

CITY OF CHARLES TOWN
FAÇADE IMPROVEMENT PROGRAM







City of Charles Town
101 E. Washington Street
Charles Town, WV 25414

Phone: 304-725-2311
www.charlestownwv.us

Investing in the Future of Charles Town

Charles Town's Façade Improvement Program is intended to assist property owners and/or tenants within the Charles Town Historic Overlay District (HOD) in beautifying and rehabilitating property fronts for the purposes of attracting both customers and prospective business owners, and serving as a tool for revitalization of the downtown area.

Those who choose to participate in this program are eligible to receive financial assistance, in the form of a 50/50 funds match, up to $7,000.00, for eligible projects and revitalization efforts in the Historic Overlay District of Charles Town. The program is managed by the City Zoning Administrator.

PROGRAM BOUNDARIES

Only properties within the boundaries of the Historic Overlay District are eligible to apply for the program.

ELIGIBLE PROJECTS

All projects accepted for the program must reflect "true to age" improvements. All improvements must be consistent with Design Review Standards established by the Charles Town Historic Landmarks Commission (CTHLC) as well as the Codified Ordinances of the City of Charles Town Codified Ordinances.

Only exterior, street-facing improvements are eligible to receive match funding. Eligible improvements include, but are not limited to:

- Awnings appropriate for the façade architecture;
- Exterior painting consistent with other downtown buildings and accepted as recognized historical coloring;
- Exterior masonry repair;
- Repair to exterior facades that face a public street;
- Sign repair;
- Repair or replacement to cornices, windows, decorative detail, doors, awnings, or window display lighting;
- Exterior lighting structures and hardware on the street-facing side of the building;
- Structural landscaping features;
- Addition or modification to entryways that allow for greater access for people with disabilities;
- Reconstruction of features that were documented to be part of the original structure;
- Removal of historically inappropriate elements or features.

INELIGIBLE PROJECTS

New construction projects, government properties, and national franchise properties are not eligible to participate in the Façade Improvement Program. Ineligible improvements include:

- Interior improvements;
- Roofing;
- Paving;
- Structural improvements;
- Security measures;
- Loading docks;
- Parking entrances;
- Removal of structurally important features.
- Installation of new signage
- Properties that have received a Façade Improvement Grant in the past 12 months, are government-owned, or are part of a national franchise are not eligible for the grant.
- Projects which do not obtain approval of a Certificate of Appropriateness (COA), if required.

Ineligible projects may be considered for approval at the discretion of City Council at their first meeting in June, provided no eligible project applications have been received by close of business on the first working day of June.

Grants are limited based on funding availability.

APPLICATION PROCESS

Each applicant will be eligible to apply for up to $7,000.00 each fiscal year. In order to be considered for a Façade Improvement Program 50/50 matching grant, the applicant shall complete the following tasks:

- Review the Design Review Standards.
- Complete and submit the Façade Improvement Program Application. If the project requires a COA the COA must first be approved by the CTHLC. If the COA is denied, no funds will be awarded.
- Submit before and after sketches, photographs, or other illustrations, and a written, detailed description of the project to be considered for the matching grant.
- Complete the property owner's or tenant's 50% matching portion of the estimated project cost and submit proposed/estimated cost. Bids must be provided if the work is being done by a contractor.

If the application and request is approved, the following will be required:

- Apply for and obtain all necessary permits.
- Submit receipts/invoices to the City once the project is complete.

POLICY FOR TWO BIDS

Two Bids will be required for any application submission. If the work is to be completed by the property owner/tenant, verification of expenses is required. The Grant does not cover the cost of labor for work done by the property owner/tenant.

APPROVAL PROCEDURES

Upon receipt of application and required materials for consideration, each application will be reviewed and the property will be deemed eligible or ineligible for grant funding by the Zoning Administrator. The decision for eligibility is based on compliance of the project with the Design Review Standards, the Codified Ordinances of the City of Charles Town, and character of the project as compared with existing properties in the surrounding area. Additionally, if the project would require a COA, the COA must be approved by the CTHLC prior to approval of the funds.

If approved for grant funding, staff will contact the applicant, and the applicant may begin their matching portion of the project, subject to permitting requirements. If the application is denied, the applicant will receive notification and an explanation of the denial.

CONDITIONS OF APPROVAL

In addition to previously listed requirements, all properties must be paid to date on all municipal taxes. Each property will be eligible for one grant per twelve (12) month period. The Zoning Administrator may add conditions of approval of the Grant application, as necessary.

PROJECT MANAGEMENT

All applicants accepted into the Façade Improvement Program will be fully responsible for managing construction of projects, including but not limited to: obtaining bids, selecting contractors, obtaining approvals, permits, and insurance; overseeing construction work, and paying all invoices for work, materials, and supplies.

Applicants shall solicit bids and proposals, materials, and labor from qualified local residents and businesses whenever possible.

In the solicitation of contractors, subcontractors, workers, and suppliers, applicants may not discriminate on the basis of: race, gender, religion, national origin, ethnicity, ancestry, origin, sexual orientation, marital status, creed, age, or disability.

The City makes no guarantees on quality and soundness of construction or other repairs, additions, or removals. Any contractor or subcontractor working on the project must be licensed and insured. In addition, any contractor or subcontractor must have a valid business license issued by the City of Charles Town. The applicant is responsible for ensuring that all contractors and subcontractors meet these requirements.

PAYMENT OF MATCHING FUNDS

Construction may begin only after the application has been approved by the Zoning Administrator, all required permits (including the COA if necessary) have been obtained, and formal approval to begin the project has been given to the applicant in writing.

Any work completed prior to formal written approval will not be eligible for funding.

Grants will be issued after the project has been completed and the City has received receipts detailing the completed work. Upon completion, City staff must be contacted for a site inspection. If the project meets all standards, the City shall provide funding for no more than 50% of the total cost of the project, not to exceed $7,000.00.

Upon completion of the project, the Applicant will provide accounting of all project costs and a copy of all paid invoices. Projects must be completed within twelve (12) months after the date of formal approval has been granted.

POLICY FOR PAINT AND MATERIALS:

Appropriate paint colors for Charles Town are color tones that would have been traditionally and predominately found in the mid-Atlantic region. Colors on a structure must be appropriate to the period from which the structure was constructed. Color tones chosen shall complement the details of the building and the composition of the color shall not obscure or hide the details.

In the event the applicant changes material or paint colors once an application is submitted, the applicant shall provide updated material to the Zoning Administrator.

FAÇADE IMPROVEMENT PROGRAM EXPIRATION DATE:

After an award of a Façade Improvement Program Grant, the awardee will have twelve months from the time of the award to complete the improvements.

Applicant's Name: _____

Application Submission Date: _____

Phone: _____

E-mail: _____

Mailing Address:_____

_____

The name of the person/entity the reimbursement check is to be made out to, and their mailing address, if different from the information provided above:

_____

_____

Project Address: _____

Have you received rebates from the City's Façade Improvement Program in the past 12 months?

☐Yes ☐No

Is this property:

New construction?	Yes	No
Government-owned property?	Yes	No
A national franchise?	Yes	No

DESCRIBE THE PROPOSED USE OF THE SUBJECT PROPERTY

_____

DESCRIPTION OF THE FAÇADE IMPROVEMENT PROJECT:

_____

_____

_____

Estimated Project **Start** Date: / / (Day / Month / Year)

Estimated Project **End** Date: / / (Day / Month / Year)

Estimated Total Project Budget: $_____

Grant Amount Requested: $_____

The following items are included with this application:

☐ Before/after sketches or photographs or illustrations

☐ Detailed proposal and/or contractor estimates

If the application and request is approved, the following will be required:

- Apply for and obtain all necessary permits.
- Submit receipts/invoices to the City once the project is complete.

CERTIFICATION

- I understand that the approved project must reflect "true to age" improvements.
- I agree to follow the plan submitted with the application and I understand that failure to do so may disqualify the project for grant funding.
- I swear and affirm that I shall not discriminate in solicitation of contractor, subcontractors, workers, or suppliers.
- I understand that an inspection of the project must be performed by City Staff upon completion of the project.
- I understand that grant monies shall not be distributed until all proposed work is completed and inspected.
- I understand that I have to provide receipts related to the project.

  For projects that involve a contractor, receipts and invoices must be accompanied by proof of payment before funds will be granted.

  If a contractor was not used, receipts must be provided to the City Staff before a reimbursement will be issued. Only materials may be reimbursed for projects that do not use a contractor.
- I agree to all of the attached "Conditions of Approval", if any, as developed by City Staff or the Historic Landmarks Commission.
- I agree to complete all improvements within one year of approval. Any time extension must be filed with and approved by City Staff.
- I have reviewed the following documents, as they pertain to my application:

  - Codified Ordinances of the City of Charles Town

  - Charles Town Historic Landmarks Commission Design Review Standards

I swear and affirm that the information provided above and within this application is accurate and correct to the best of my knowledge. I also assure that the property listed is in compliance with all laws, ordinances, rules, and regulations of the State of West Virginia and the City of Charles Town:

Property Owner's **Signature**: _____

Date: _____

Applicant's **Signature**: _____

Date: _____

Please submit an original completed petition to the following:

Zoning Administrator

City of Charles Town

101 E. Washington Street Charles Town, WV 25414

FOR CITY USE ONLY

Application Number:_____ Date Application Received:_____

Zoning District: _____

Zoning Administrator Approval:_____ Date:_____

Historic Landmarks Commission Approval:_____Date:_____

Amount awarded: $_____

Comments:

_____

_____

_____

_____

_____

_____

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Resolution
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2046: Updated Opioid Fund Resolution

ATTACHMENTS:

- Updated Grant Funds Resolution.pdf
- 2025-005 - Resolution Allocating Opioid Funds to Police Social Work Program.pdf

A RESOLUTION OF THE CITY OF CHARLES TOWN, WEST VIRGINIA, ALLOCATING OPIOID FUNDS TO THE POLICE SOCIAL WORK PROGRAM

WHEREAS, the City Council is the recipient of Opioid Settlement Funds intended to combat the opioid crisis and the lasting impacts of opioid addiction on the community and its citizens; and

WHEREAS, the Council has considered the best approach to utilize these funds in a manner that will provide the maximum benefit to the City; and

WHEREAS, the City, pursuant to the guidelines established by the State of West Virginia, has approved the following purposes for which Opioid Funds can be used: (1) evidence-based strategies, programming, and/or services used to expand the availability of treatment for individuals affected by substance use disorders or addiction; (2) developing, promoting, and providing evidence-based substance use prevention strategies; (3) providing substance use avoidance and awareness; (4) engaging in enforcement or curtailing the sale, distribution, promotion, or use of opioids and other drugs; (5) decreasing the oversupply of licit and illicit opioids; and (6) supporting recovery from addiction to be performed by qualified providers; and

WHEREAS, the Charles Town Police Department has been at the forefront of the opioid epidemic and currently provides services directly related to combating illicit opioid use; and

WHEREAS, the Police Department has been faced with calls for service involving individuals experiencing substance abuse issues, homelessness, and other complex social and behavioral health needs related to opioid use; and

WHEREAS, police officers are often the first responders to these situations but may not always have the specialized training or resources to handle them effectively, and the involvement of unarmed social workers in such situations can promote better outcomes; and

WHEREAS, collaboration between police officers and social workers has been shown to reduce police officers' time spent on non-criminal calls, improve crime victim cooperation, and strengthen police-community relationships; and

WHEREAS, the City Council previously allocated $75,000.00 in Opioid Funds to establish a social worker position in collaboration with the Martinsburg Initiative for one year beginning July 1, 2025; and

WHEREAS, on July 7, 2025, the City Council allocated funds to fund the police social worker in succeeding fiscal years; and

DRAFT

WHEREAS, the Charles Town Initiative, which sponsors the police social worker in the Charles Town Police Department, has been awarded a grant that will fund the social worker for the next four years, beginning in November 2026; and

WHEREAS, since its inception, the Charles Town police social work program has proven effective in combating the opioid crisis and has achieved enhanced results through collaboration with Charles Town Police Department; and

WHEREAS, in light of the recent grant award, the City Council desires to allocate the remaining funds in the FY 26 fiscal year to support the needs of the current police social worker and to allocate additional funds in future fiscal years to support expansion of the police social work program**;**

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF CHARLES TOWN, WEST VIRGINIA:

1. **Current fiscal year:** That the City Council of Charles Town hereby allocates the remaining Opioid Funds in the current fiscal year to support the needs of the current police social worker in the Charles Town Police Department.

2. **Subsequent Funding:** That the City Council will allocate additional Opioid Funds in future fiscal years to support the expansion of the police social work program.

ADOPTED this _____ day of _____, 2026.

Attest:

_____ _____

Michael George
Mayor

Alissa Meeks
City Clerk

DRAFT

City of Charles Town
101 East Washington Street, P.O. Box 14, Charles Town, WV 25414
Phone: (304) 725-2311 ♦ Web: www.charlestownwv.us

RESOLUTION ALLOCATING OPIOID FUNDS TO POLICE SOCIAL WORK PROGRAM

WHEREAS, the City Council is the recipient of Opioid Settlement Funds intended to combat the opioid crisis and the lasting impacts of opioid addiction on the community and its citizens; and

WHEREAS, the Council has considered the best approach to utilize these funds in a manner that will provide the maximum benefit to the City ; and

WHEREAS, the City, pursuant the guidelines established by the State of West Virginia, has approved the following purposes for which OPIOID funds can be used: 1)Evidence based strategies, programming, and/or services used to expand the availability of treatment for individuals affected by substance use disorders or addiction. 2) To develop, promote, and provide evidence-based substance use prevention strategies, 3) To provide substance use avoidance and awareness, 4)To engage in enforcement or curtail the sale, distribution, promotion, or use of opioids and other drugs, 5) To decrease the oversupply of licit and illicit opioids, and 6) To support recovery from addiction to be performed by qualified providers; and

WHEREAS, the City Police Department has been at the forefront of the opioid epidemic and currently provides services directly related to combating illicit opioid use; and

WHEREAS, the Police Department has been faced with calls for service involving individuals experiencing substance abuse issues, homelessness, and other complex social and behavioral health needs, related to opioid use; and

WHEREAS, police officers are often the first responders to these situations but may not always have the specialized training or resources to handle them effectively, and the involvement of unarmed social workers in such situations can promote better outcomes; and

WHEREAS, collaboration between police officers and social workers has been shown to reduce police officers' time spent on non-criminal calls, improve crime victim cooperation, and strengthen police-community relationships; and

WHEREAS, the Martinsburg Initiative, a program founded in adjacent Berkeley County, has proven effective in combating the opioid crisis and has achieved enhanced results through collaboration with law enforcement agencies; and

WHEREAS, the Martinsburg Initiative seeks to expand its program to additional municipalities and counties, but requires additional funding to facilitate this expansion.

NOW THEREFORE LET IT BE RESOLVED that the City Council of Charles Town hereby allocates Opioid Funds in the amount of $75,000.00 to the City Police Department for the purpose of establishing a social worker position in collaboration with Martinsburg Initiative for one year, beginning on July 1, 2025;

NOW, THEREFORE, BE IT FURTHER RESOLVED that the City Council allocates the remaining funds to a reserve account for potential funding for the police social work program in future years, subject to an analysis of the program's financial requirements and an evaluation of the program's effectiveness following its first year of implementation.

Adopted this 21st day of July, 2025.

Attest:

Michael George
Mayor

Carolyn Vezzosi
Deputy City Clerk

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2047: City Service Fee on New Construction Discussion - Possible Executive Session

Alternative Proposed Motion:

ATTACHMENTS:

- Developer Fee Council Packet.pdf
- FINAL REPORT.pdf
- Subdivision Proffers.pdf
- W Va Code 8-13-13.pdf
- Ranson City Service fee 1.docx

CITY OF CHARLES TOWN

CITY COUNCIL

AGENDA • APRIL 28, 2022

Special | **Council Chambers** | **9:30 AM**

101 East Washington Street, Charles Town, WV 25414

I. CALL TO ORDER

II. UNFINISHED BUSINESS

III. NEW BUSINESS

1. 5597: DTA Developer Fee

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 04/28/22 09:30 AM
Department: City Council
Category: Recommendation
Initiator: Carolyn Vezzosi

SCHEDULED

AGENDA ITEM (ID # 5597)

DTA Developer Fee

Mayor's Select Committee for Developer Fee analysis - Review draft versions of DTA's analysis and provide feedback to DTA.

ATTACHMENTS:

- Executed copy of DTA Agreement (PDF)
- Executed Copy of DTA Agreement (PDF)
- MayorSelectCommittee_DevFees_15Mar2022 (PDF)
- Preliminary Fee range estimates (PDF)
- Memo Population 03.18.22 .v5 (PDF)
- Charles Town Fee Memo 4.18.22 v1 with Capital project calculations (PDF)
- Public Facilities Needs List 2040 (PDF)
- Executed copy of DTA Agreement (PDF)

dta

www.FinanceDTA.com

AGREEMENT FOR CONSULTING SERVICES

CITY OF CHARLES TOWN

ASSESSMENT OF MUNICIPAL DEVELOPER FEES

October 4, 2021

Public Finance
Public-Private Partnerships
Development Economics
Clean Energy Bonds

Newport Beach | San Jose | San Francisco | Riverside
Dallas | Houston | Raleigh | Tampa

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

AGREEMENT FOR CONSULTING SERVICES

THIS AGREEMENT is made and entered into this 12th day of October of 2021, by and between the City of Charles Town at 101 East Washington Street, Charles Town, WV 25414, herein called "City" or "Client," and DTA at 5000 Birch Street, Suite 3000, Newport Beach, CA 92660, herein after called "DTA" or "Consultant." The Client and the Consultant in consideration of the mutual promises and conditions herein contained agree as follows.

ARTICLE I
DISCLOSURES AND TERM OF CONTRACT

Section 1.1 As of the date of this Agreement, there are no actual or potential conflicts of interest that DTA is aware of that might impair its ability to render unbiased and competent advice or to fulfill its fiduciary duty. If DTA becomes aware of any potential conflict of interest that arise after this disclosure, DTA will disclose the detailed information in writing to the Client in a timely manner.

Section 1.2 DTA, a Securities and Exchange Commission ("SEC") and MSRB registered firm, does not have any legal events and disciplinary history on its Form MA and Form MA-I, which includes information about any criminal actions, regulatory actions, investigations, terminations, judgments, liens, civil judicial actions, customer complaints, arbitrations and civil litigation. The Client may electronically access DTA's most recent Form MA and each most recent Form MA-I filed with the Commission at the following website:

https://www.sec.gov/edgar/searchedgar/companysearch.html

Section 1.3 This agreement shall become effective on the date stated above and will continue in effect until the earlier of (i) that day when the services provided for herein have been performed or (ii) until terminated as provided in Article 6 below.

ARTICLE II
SERVICES TO BE PERFORMED BY CONSULTANT

Section 2.1 Consultant agrees to perform the professional services for the Client for the assessment of Municipal Developer Fees, herein after called "Project" in accordance with the applicable professional standard of care and to deliver the work products to the Client as described in the Scope of Work statement attached as Exhibit "A" hereto. Such professional services and work products, as from time to time modified in accordance with Section 2.3 hereof, are collectively referred to as the "Consulting Services."

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

Section 2.2 Instruments of Service. All computer software (including without limitation financial models, compilations of formulas and spreadsheet models), inventions, designs, programs, improvements, processes and methods (collectively, the "Proprietary Models"), reports, drawings, specifications, computer files, field data, notes and other documents and instruments prepared by Consultant are Instruments of Service of Consultant and shall remain the property of Consultant. Consultant shall likewise retain all common law, statutory and other reserved rights, including the copyright thereto. Client acknowledges and agrees that the consideration paid by Client herein only entitles Client to a license to use the hard copy or electronically transmitted reports generated pursuant to the Consulting Services and that any Proprietary Model that Consultant uses to generate such reports is owned by, or is duly licensed from a third party to Consultant and is not being provided to Client hereunder. The reports and models used to generate such reports are for use on this Project only. The Client shall not reuse or make any modification to the hard copy or electronically transmitted reports generated pursuant to the Consulting Services without the prior written authorization of the Consultant. The Client agrees, to the fullest extent permitted by law, to indemnify and hold harmless the Consultant, its shareholders, officers, directors, employees and subconsultants (collectively, Consultant's) against any damages, liabilities or costs, including reasonable attorneys' par fees and defense costs, arising from or allegedly arising from or in any way connected with the unauthorized use, reuse or modification of the hard copy or electronically transmitted reports generated pursuant to the Consulting Services or any of Consultant's Instruments of Service, including models, by the Client or any person or entity that acquires or obtains the reports from or through the Client without the written authorization of the Consultant. Client acknowledges that Consultant may have used reports and analyses that Consultant authored for other clients as base works or templates for the reports and analyses prepared for Client pursuant to this Agreement, and Client acknowledges and agrees that Consultant has the right to use the reports and analyses that it authors pursuant to this Agreement as base works or templates for reports and analyses that Consultant authors for Consultant's other clients, provided, however that Consultant shall not use any confidential information provided by Client in such future reports and analyses. Client further acknowledges and agrees that Consultant has spent substantial time and effort in collection and compiling data and information (the "Data Compilations") in connection with the Consulting Services and that such Data Compilations may be used by Consultant for its own purposes, including, without limitation, sale or distribution to third parties; provided, however, that Consultant will not sell or distribute any of Client's confidential information that may be contained in such Data Compilations, unless such confidential information is used only on an aggregated and anonymous basis.

Section 2.3 Any proposed changes in the Consulting Services hereunder shall be submitted to the other party hereto, and any such changes agreed to by the parties shall be reflected in an amendment to Exhibit "A" in accordance with Section 7.2 hereto.

Section 2.4 Nothing in this Agreement shall give the Consultant possession of authority with respect to any Client decision beyond the rendition of information, advice, recommendation, or counsel.

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

ARTICLE III
COMPENSATION

Section 3.1 Client agrees to pay Consultant for its Consulting Services in accordance with this Agreement, a professional fee computed according to the Professional Fee Schedule attached as Exhibit "B" hereto and incorporated herein by reference (the "**Fee Schedule**"). Client acknowledges and agrees that portions of Consultant's professional fees and expenses may have been incurred by Consultant prior to the execution of this Agreement (the "**Pre-Agreement Fees**") and Client agrees to pay such Pre-Agreement Fees in accordance with this Agreement.

Section 3.2 The Client shall reimburse the Consultant for out-of-pocket and administrative expenses by paying a charge equal to 3% of DTA's monthly billings. Expenses shall include all actual expenditures made by Consultant in the performance of any Consulting Services undertaken pursuant to the Agreement, including, without limitation, the following expenditures:

(a) Cost of clerical assistance, including typing, collation, printing and copying, plus copier and photography costs, including photographic reproduction of drawings and documents.

(b) Transportation costs, including mileage for the use of personal automobiles at the prevailing IRS standard rate, rental vehicles, lodging and regularly scheduled commercial airline ticket costs.

(c) Courier services, facsimile, and telephone expenses.

Section 3.3 On or about the first two weeks of each month during which Consulting Services are rendered hereunder, Consultant shall present to Client an invoice covering the current Consulting Services performed and the reimbursable expenses incurred pursuant to this Agreement and exhibits thereto. Such invoices shall be paid by Client within thirty (30) days of the date of each invoice. A 1.2% charge may be imposed against accounts which are not paid within 30 days of the date of each invoice.

Section 3.4 The maximum total fee amount set forth in Exhibit "B" may be increased as a result of any expansion of the Consulting Services to be rendered hereunder pursuant to Section 2.3 or as provided in Exhibit "A" hereto.

Section 3.5 Records of the Consultant's costs relating to (i) Consulting Services performed under this Agreement and (ii) reimbursable expenses shall be kept and be available to the Client or to Client's authorized representative at reasonable intervals during normal business hours.

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

ARTICLE IV
OTHER OBLIGATIONS OF CONSULTANT

Section 4.1 Consultant agrees to perform the Consulting Services in accordance with Exhibit "A" and the applicable standard of care. Should any errors caused by Consultant's negligence be found in such services or products, Consultant will correct them at no additional charge by revising the work products called for in Exhibit "A" to eliminate the errors.

Section 4.2 Consultant will supply all tools and instrumentalities required to perform the Consulting Services under the Agreement.

Section 4.3 Neither this Agreement nor any duties or obligations under this Agreement may be assigned by Consultant without the prior written consent of Client. However, Consultant may subcontract portions of the work to be performed hereunder to other persons or concerns provided Consultant notifies Client of the name and address of said proposed subcontractor and Client either consents or fails to respond to notification with respect to the use of any particular proposed subcontractor.

Section 4.4 In the performance of its Consulting Service hereunder, Consultant is, and shall be deemed to be for all purposes, an independent contractor (and not an agent, officer, employee or representative of Client) under any and all laws, whether existing or future. Consultant is not authorized to make any representation, contract, or commitment on behalf of Client.

ARTICLE V
OTHER OBLIGATIONS OF CLIENT

Section 5.1 The Client shall provide full information in a timely manner regarding requirements for and limitations on the Project. Client agrees to comply with all reasonable requests of Consultant and provide access to all documents reasonably necessary to the performance of Consultant's duties under this Agreement with the exception of those documents which Exhibit "A" calls upon the Consultant to prepare.

Section 5.2 Neither this Agreement nor any duties or obligations under this Agreement may be assigned by Client without the prior written consent of Consultant.

Section 5.3 The Client shall provide prompt written notice to the Consultant if the Client becomes aware of any fault or defect in the Project, including any errors, omissions, or inconsistencies in the Consultant's Instruments of Service.

Section 5.4 Client, public agencies, landowners, consultants and other parties dealing with Client or involved in the subject development project referred to in Exhibit "A"

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

will be furnishing to Consultant various data, reports, studies, computer printouts and other information and representations as to the facts involved in the project which Client understands Consultant will be using and relying upon in preparing the reports, studies, computer printouts and other work products called for by Exhibit "A." Consultant shall not be obligated to establish or verify the accuracy of the information furnished by or on behalf of Client, nor shall Consultant be responsible for the impact or effect on its work products of the information furnished by or on behalf of Client, in the event that such information is in error and therefore introduces error into Consultant's work products.

Section 5.5 In the event that court appearances, testimony or depositions are required of Consultant by Client in connection with the services rendered hereunder, Client shall compensate Consultant at a rate of $400 per hour and shall reimburse Consultant for out-of-pocket expenses on a cost basis.

ARTICLE VI
TERMINATION OF AGREEMENT

Section 6.1 Either party may terminate or suspend this Agreement upon thirty (30) days written notice. Unless terminated as provided herein, this Agreement shall continue in force until the Consulting Services set forth in Exhibit "A" have been fully and completely performed and all proper invoices have been rendered and paid.

Section 6.2 Should either party default in the performance of this Agreement or materially breach any of its provisions, the other party at its option may terminate this Agreement by giving written notification to the defaulting party. Such termination shall be effective upon receipt by the defaulting party, provided that the defaulting party shall be allowed ten (10) days in which to cure any default following receipt of notice of same.

Section 6.3 In the event of any termination that is not the fault of the Consultant, the Client shall pay the Consultant, in addition to payment for services rendered and reimbursable costs incurred, for all expenses reasonably incurred by the Consultant in connection with the orderly termination of this Agreement, including but not limited to demobilization, reassignment of personnel, associated overhead costs and all other expenses directly resulting from the termination, plus an amount for the Consultant's anticipated profit on the value of the services not performed by the Consultant.

Section 6.4 Suspension and Termination for Non-Payment. (i) In addition to any other provisions in this Agreement regarding breach of the Agreement, if the Client fails to make payments when due, the Consultant may suspend performance of services upon ten (10) calendar days' notice to the Client. The Consultant shall have no liability whatsoever to the Client for any costs or damages as a result of such suspension caused by any breach of this Agreement by the Client. Upon payment in full by the Client, the Consultant shall resume services under this Agreement, and the time schedule and compensation shall be

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

equitably adjusted to compensate for the period of suspension plus any other reasonable time and expense necessary for the Consultant to resume performance. (ii) If the Client fails to make payment to the Consultant in accordance with the payment terms herein, and/or Client has failed to cure its breach or default following a suspension of services as set forth above, this shall constitute a material breach of this Agreement and shall be cause for termination of this Agreement by the Consultant upon seven (7) days written notice to the Client. (iii) Payment of invoices shall not be subject to any discounts or set-offs by the Client, unless agreed to in writing by the Consultant. Payment to the Consultant for services rendered and expenses incurred shall be due and payable regardless of any subsequent suspension or termination of this Agreement by either party.

Section 6.5 The covenants contained in Sections 3.1, 3.2, 4.4, 5.3, 5.4 and all of Article VII shall survive the termination of this Agreement.

ARTICLE VII
GENERAL PROVISIONS

Section 7.1 Any notices to be given hereunder by either party to the other may be affected either by personal delivery in writing or by mail. Mailed notices shall be addressed to the parties at the addresses appearing in the introductory paragraph of this Agreement, but each party may change the address by written notice in accordance with the first sentence of this Section 7.1. Notices delivered personally will be deemed communicated as of actual receipt. Mailed notices will be deemed communicated as of two (2) days after mailing.

Section 7.2 This Agreement and exhibits hereto supersede any and all agreements, either oral or written, between the parties hereto with respect to the rendering of service by Consultant for Client and contains all of the covenants and agreements between the parties with respect to the rendering of such services. Each party to this Agreement acknowledges that no representations, inducements, promises, or agreements, orally or otherwise, have been made by any party, or anyone acting on behalf of any party, which are not embodied herein, and that no other agreement, statement, or promise not contained in this Agreement shall be valid or binding. Any modification of this Agreement (including any exhibit hereto) will be effective if it is in writing and signed by the party against whom it is sought to be enforced.

Section 7.3 If any provision in this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions will nevertheless continue in full force without being impaired or invalidated in any way.

Section 7.4 Disputes. The parties agree to first try in good faith to settle the dispute by mediation pursuant to the Mediation Rules of the American Arbitration Association. If the claim or controversy is not settled by mediation, the claim or controversy may be

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

resolved by final and binding arbitration. On the written request of one party served on the other, the dispute shall be submitted to binding arbitration in accordance with the commercial rules and regulations of the American Arbitration Association and the provisions of the California Arbitration Act (Sections 1280 through 1294.2 of the California Code of Civil Procedure). The arbitration shall take place in Newport Beach, California, or such other location mutually agreed to by the parties.

The arbitrator(s) shall be selected as follows: In the event that Consultant and Client agree on one arbitrator, the arbitration shall be conducted by such arbitrator. In the event Consultant and Client do not so agree, Consultant and Client shall each select an arbitrator and the two arbitrators so selected shall select the third arbitrator. If there is more than one arbitrator, the arbitrators shall act by majority vote. The parties may propose arbitrators from JAMS, ADR, ARC or any independent arbitrator/neutral for dispute resolution. The parties are not required to hire a AAA arbitrator for resolution of a dispute hereunder.

No arbitration shall include by way of consolidation or joinder any parties or entities not a party to this Agreement without the express written consent of the Client, the Consultant and any party or entity sought to be joined with an express reference to this provision. Any party or entity joined in the arbitration, after mutual consent, shall be bound by this provision.

The decree or judgment of an award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

Section 7.5 The prevailing party in any arbitration or legal action brought by one party against the other and arising out of this Agreement shall be entitled, in addition to any other rights and remedies it may have, to reimbursement for its expenses, including court costs and reasonable attorneys' fees. The non-prevailing party shall be liable, to the extent allowable under law, for all fees and expenses of the arbitrator(s) and all costs of the arbitration.

Section 7.6 This Agreement will be governed by and construed in accordance with the laws of the State of California.

Section 7.7 Nothing contained in this Agreement shall create a contractual relationship with or a cause of action in favor of a third party against either the Client or the Consultant. The Consultant's services under this Agreement are being performed solely for the Client's benefit, and no other party or entity shall have any claim against the Consultant because of this Agreement or the performance or nonperformance of services hereunder.

Section 7.8 Notwithstanding any other provision of this Agreement, and to the fullest extent permitted by law, neither the Consultant nor the Client, their respective officers, directors, partners, employees, contractors or subconsultants shall be liable to the other for, or shall make, any claim for any incidental, indirect or consequential damages

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

arising out of or connected in any way to the Project or to this Agreement. This mutual waiver of consequential damages shall include, but is not limited to, loss of use, loss of profit, loss of business, loss of income, loss of reputation or any other consequential damages that either party may have incurred from any cause of action including negligence, strict liability, breach of contract and breach of strict or implied warranty.

Section 7.9 It is intended by the parties to this Agreement that the Consultant's services in connection with the Project shall not subject the Consultant's individual shareholders, officers, directors, members, managers or employees to any personal legal exposure for the risks associated with this Project. Therefore, and notwithstanding anything to the contrary contained herein, Client agrees that as Client's sole and exclusive remedy, any claim, demand or suit shall be directed and/or asserted only against Consultant and not against any of the individual shareholders, officers, directors, members, managers or employees.

Section 7.10 Limitation of Liability – for available insurance: In recognition of the relative risks and benefits of the Project to both the Client and the Consultant, the risks have been allocated such that the Client agrees, to the fullest extent permitted by law, to limit the liability of the Consultant to the Client for any and all claims, losses, costs, damages of any nature whatsoever or claims expenses from any cause or causes, including attorneys' fees and costs and expert-witness fees and costs, so that the total aggregate liability of the Consultant to the Client shall not exceed the sum of insurance coverage available at the time of settlement or judgment. It is intended that this limitation apply to any and all liability or cause of action however alleged or arising, except for Consultant's willful misconduct or unless otherwise prohibited by law.

IN WITNESS WHEREOF, this Agreement has been executed on the date and year first above written.

CONSULTANT:
David Taussig and Associates, Inc.
d/b/a DTA

By: _____
Nathan Perez, Managing Director

Date: 10/14/2021

CLIENT:
City of Charles Town

By: _____

Date: 12 Oct 2021

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

SCOPE OF WORK

Work products stemming from the work plan described in this section will include a memorandum ("memo") summarizing the fee methodology options and the Draft and Final Administrative Reports.

DTA's clients receive high levels of personal attention from senior staff, with a Principal, Senior Vice President, or Vice President always available to meet with public agency staff and other groups. **Notably, the firm shall provide ongoing communication, education, and outreach throughout the duration of the project.**

Task 1 – Development of Project Strategy and Kickoff Meeting

DTA staff will meet with City staff in a project kickoff meeting to finalize the details of the project, deliverables, timetables, and tasks, discuss the fee methodologies and best practices, identify needed information (i.e., reports, project/needs lists, stakeholder groups, data, etc.), prepare the final schedule, discuss the public process, and resolve other concerns, as appropriate.

Task 2 – Develop Population and Dwelling Unit Projections

DTA will compile and document existing and future population and development estimates for the City. The projections resulting from this task will ultimately calculate fee levels. At this stage, DTA will evaluate City resources, influences, all factors affecting the existing Fee Study, and pertinent impact fees as outlined by the City. This task comprises four subtasks.

2A **Population Projections**: DTA will gather existing information on present and future population for the City from various sources, including City staff, the County Assessor's Office parcel database, the General Plan, the Comprehensive Plan, existing Master Plans, the Capital Improvements Plan, the U.S. Census, the Finance Division of the West Virginia Department of Administration, and from other data sources, as needed.

2B **Conduct Entitlement Research and Projections**: DTA will coordinate with City staff to determine existing and future residential and non-residential development within the City over the planning horizon. To complete this subtask, DTA will review the General Plan/Capital Improvements Plan and related plans to determine expected development land use patterns in the City, assess City records to identify existing entitlements for dwelling units and commercial/industrial development, and project the number of new dwelling units and commercial/industrial development based on existing entitlements and population projections through 2035, or such other target year as selected by City staff.

2C **Review Current City Fee Structure**: DTA shall review and summarize the City's current development fee structures, City policies and procedures, and other regulatory requirements affecting potential fee structures and revenue program requirements.

2D **Review Prior City Fee Justification Studies**: DTA shall review the approach and methodology utilized in prior City fee justification studies so they can be evaluated in

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

light of the City's current needs.

Task 3 – Review Facility/Capital Needs and Levels of Service

This task entails the review of the facilities and capital needs required to serve new development in the study area projected in Task 2. DTA will use existing City materials (and any relevant Developer's Facilities Reports) as base documents and focus our effort on updating this information.

For any fee program to be comprehensive in its scope, it is necessary to complete a thorough identification and review of all the facilities that will be impacted by additional growth, including those already discussed in the General Plan or Capital Improvements Plan. This task will require close coordination with all appropriate City departments.

3A **Survey/Interview City Staff**: DTA shall survey/interview City staff to review projected facilities in the City, along with major equipment needs, the timing at which improvements will be needed, and any physical data that would assist in developing the costs estimated below in Subtask 3C. Based upon the results of the surveys and interviews, DTA will verify and, if appropriate, expand the list of new facilities found in the General Plan or Capital Improvements Plan to be included within the fee program for the City.

3B **Facilities List**: Based on the information collected in Subtask 3A, DTA shall prepare a facilities needs list that details the new facilities and equipment to serve new development in the City.

3C **Review Cost Estimates**: DTA's engineering and technical staff will, as necessary, consult with City department heads and/or engineering staff or equivalent to ascertain and understand in-house cost data for existing and projected facilities and equipment, apply inflation and cost-of-living escalators to the list of projected public facilities to determine future costs, review and/or refine existing cost data, examine major sources of revenue to fund the construction of new public facilities, and provide a proportional estimate between projected costs for new facilities and estimated revenue from mitigation fees and other sources.

Task 4 – Develop Methodology for Calculating New Fee Amounts

This task entails developing the methodology used to establish the fee amount for each fee component to the extent appropriate. There are two critical issues that must be considered in developing a fee program. The fee program must generate revenues in a timely manner and the methodology must meet the nexus or benefit requirements of the Impact Fees Act. Since fees of any sort are controversial, it is critical that any fee established be legally defensible.

DTA's Fee Study methodology must meet the nexus or benefit requirements of the Impact Fees Act, which requires that there be a nexus between the fees imposed, use of the fees, and development projects on which the fees are imposed. Furthermore, there must be a relationship between the amount of the fee and cost of the improvements.

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

Implicit in these requirements is a stipulation that a public agency cannot impose a fee to cure existing deficiencies in public facilities or improve public facilities beyond what is required based on the specific impacts of new development. The benefit methodology established in this task will be documented in the Final Report.

DTA will recommend a Fee Expenditure Plan to ensure that projects can be fully funded and implemented within any required time limits for expenditures of such funds and possible flexibility to allow collected fees to be used to provide the City with a match for grant applications. Finally, the memo will include recommendations for methodology and next steps. Upon review and discussion by City staff, a methodology will be selected.

Deliverable: Memo Summarizing the Fee Methodology Options

Task 5 – Determine Fee Levels and Generate Cash Flow Analysis

This task entails calculating the fee amounts based upon the dwelling unit and commercial/industrial development projections completed in Task 2, facilities needs and costs determined in Task 3, and methodology selected in Task 4.

5A **Calculate Recommended Fee Amounts**: DTA shall calculate fees for the City by inputting the data compiled under the preceding tasks and computing each fee to be levied. This work will be done in a spreadsheet format that can be updated annually. DTA will also evaluate this data in comparison to surrounding cities so as to arrive at comparable and palatable fee levels.

5B **Document Fee Derivation**: DTA shall document the methodology utilized for the fee calculation model that can be understood by the City and public. DTA shall prepare written statements documenting the validity of the methodology for deriving each of the fees for the City. These statements will be made to meet the requirements of the Impact Fees Act and documented in the Final Report discussed below.

Task 6 – Prepare Draft and Final Reports

This task entails the preparation of the Draft and Final Reports for consideration by the City Council and City staff.

6A **Prepare Draft Report for Comments**: Based on the work completed in Tasks 1-5, DTA will prepare the Draft Report for review and consideration by City staff. The Draft Report will be prepared under the standards of the Impact Fees Act and is expected to include an executive summary, population projections, a facilities and improvements list, areas of benefit (if applicable), fee calculations, recommended fee levels, and the suggested process for keeping fees current.

6B **Prepare Final Report**: Based on the incorporation of City staff comments and concerns on the Draft Report, DTA will prepare the Final Report for presentation to the City Council and City staff.

Deliverable: Draft and Final Reports

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

Task 7 – Outline Tasks Required for the Implementation and Administration of the Fee Program

DTA will prepare a list of tasks required of the City once they have adopted their new fee program. These tasks include the determination of actual fee levels if the City decides not to impose the maximum fee levels allowed under the Fee Study, the implementation of the fee credit program, and other issues the City may face when carrying out the fee program. In addition, DTA shall prepare a Draft Ordinance to adopt the fee program, subject to review and approval by the City's legal counsel.

Task 8 – Attend Meetings and Public Outreach

This task entails attendance at a total of four (4) meetings/workshops, including the kickoff meeting, with the City Manager, the Community Development Team, other City leadership and staff, focus groups, stakeholders, and the City Council to present information regarding the status of the impact fee program update, draft study, and Final Report to obtain input. DTA will also be prepared to lead meetings and workshops with selected groups to gain better project understanding, gauge community sentiment, and determine the key objectives. During these meetings, DTA will consider community and stakeholder input. For this purpose, DTA will develop handouts for these meetings that summarize the findings and analysis from the Public Review Draft.

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

FEE SCHEDULE

Fees for services shall be charged on an hourly basis according to the rates set forth in the **fee schedule** below, with invoices being submitted to the City monthly. The estimated fee for services is not to exceed **$48,000** for the Fee Study, excluding out-of-pocket expenses. Further work at that point would require additional fees.

Table 1: Proposed Budget

Type of Fee	Percentage Allotted	Estimated Cost
Fire and Rescue	15%	$7,200.00
Municipal Facilities	15%	$7,200.00
Library	15%	$7,200.00
Parks and Recreation	15%	$7,200.00
Police	15%	$7,200.00
Transportation (Connectivity)	25%	$12,000.00
Total	**100%**	**$48,000.00**

Table 2: DTA's Fee Schedule

Labor Category	Labor Rate
President/Managing Director	$290/Hour
Senior Vice President	$260/Hour
Vice President	$240/Hour
Senior Manager	$205/Hour
Manager	$195/Hour
Senior Associate	$185/Hour
Associate III	$175/Hour
Associate II	$165/Hour
Associate I	$150/Hour
Research Associate II	$140/Hour
Research Associate I	$125/Hour

Additional meetings [more than the four (4) meetings specified in the Scope of Work, including two (2) virtual meetings and two (2) in-person meetings] shall be charged at the rate of $2,500 per in-person meeting. DTA staff shall also schedule standing conference calls (i.e., weekly or bi-weekly) with City staff to stay on track with tasks and deliverables.

Out-of-pocket and administrative expenses shall be equal to 3% of DTA's billings for labor, plus travel expenses and any outside vendor payments, not to exceed $2,000. All hourly rates for services apply through December 31, 2021, and are subject to a cost-of-living increase.

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

www.FinanceDTA.com

A Limitations

The labor costs in the table above include attendance at a total of four (4) formal meetings with City staff, stakeholders, the Community Development Team, and the City Council, including the kickoff meeting. Attendance at more than four (4) meetings, detailed written responses to resolve disputes, or the preparation of more than one set of major revisions to the Draft Report will be classified as additional work and may require further billing at the hourly rates identified in Table 2 if the maximum fee levels have been exceeded.

Other examples of additional work shall include:

- Additional analyses based on revised assumptions requested by the City, including possible changes in the facilities needs list, infrastructure costs, population projections, and related data once the preparation of the Draft Report has been initiated and/or adjustments to assumptions once the Draft Report has been approved;
- Meetings shall be conducted virtually via an online meeting software, where possible;
- Negotiations with stakeholders once the Final Report has been prepared;
- Time expended related to obtaining data assigned to the City under "Information to be Provided by the City";
- Actual implementation of the fee program; and
- Reproduction of more than five bound copies of the Final Report.

The maximum fees listed above assume the review and implementation of the fee program with a schedule between the initiation of services and public outreach that is within the proposed time frame according to the City's specifications.

Attachment: Executed Copy of DTA Agreement (5597 : DTA Developer Fee)

OFFICE OF THE MAYOR

ROBERT M. TRAINOR

The Golden Rule City

15 March 2022

Subj: Mayor's Select Committee on the Assessment of Charles Town Developer Fees

Dear Council members

Please be advised that I have commissioned a Select Committee to provide support to City staff in the execution of the contract to assess Charles Town's developer fees. The primary purpose of the assessment is to:

1) Identify present and future capital projects and expenses that will be borne by Charles Town resulting from development;
2) Determine the appropriate developer fee amount for Charles Town to meet those projected expenses; and
3) Provide for the consistent application and review of developer fees throughout Charles Town.

The following Council Members are hereby appointed to the Select Committee:

- Mr. Robert Trainor, Mayor & Finance Committee Chair
- Ms. Jean Petti, Ward 3 Rep & Finance Committee Member
- Mr. Jeff Hynes, Ward 2 Rep & Finance Committee Member
- Ms. Elizabeth Ricketts, Ward 1 Rep & Infrastructure Committee Member

All Committee meetings will conform with applicable ordinances, rules, and regulations.

Robert M. Trainor
Mayor

101 E. WASHINGTON STREET, CHARLES TOWN, WV 25414

Attachment: MayorSelectCommittee_DevFees_15Mar2022 (5597 : DTA Developer Fee)

dta
www.FinanceDTA.com

MEMORANDUM

April 21, 2022

To: Alissa Meeks, City of Charles Town WV

From: DTA Inc.

Subject: Preliminary Municipal Developer Fee Estimates Update.

DTA has updated this memorandum to present the preliminary Municipal Developer Fees (the "Fees") to the City of Charles Town. (the "City"). **Tables 1 through 3,** shown below, summarizes the preliminary Municipal Developer fees for six (6) fee categories. DTA has based these preliminary fee estimations on the 2021 demographic and land use numbers approved by the City staff. The fee schedule is based on the City's Growth Related Capital Improvement Projects – Developer Fee Analysis as of November 30, 2021. In this memorandum, DTA added $75,000 to the Transportation facilities total to account for the "Feasibility Study to examine options for connecting Wards 2 and 4 to downtown." DTA has presented three specific fee schedule scenarios; Lowest Project Costs, Midrange Project Costs and Highest Project Costs.

Table 1: Lowest Cost Proposed Municipal Developer Fees

Land Use	Fire	Police	Municipal	Library	Parks	Transportation	Total
Single Family	$105	$169	$928	$62	$499	$792	$2,556
Multi-Family	$105	$167	$921	$62	$495	$352	$2,102
Commercial	$47	$75	$414	$0	$0	$2,010	$2,546
Office	$49	$79	$436	$0	$0	$1,200	$1,764
Industrial	$28	$44	$244	$0	$0	$412	$728
Institutional	$32	$33	$184	$0	$0	$624	$873

Note:

1. Growth related capital improvement project total $15,275,000
2. City Hall expansion / renovation costs $3.0 million
3. West End Gateway costs $4.0 million.

Table 2: Midrange Cost Proposed Municipal Developer Fees

Land Use	Fire	Police	Municipal	Library	Parks	Transportation	Total
Single Family	$105	$169	$1,140	$62	$499	$894	$2,868
Multi-Family	$105	$167	$1,130	$62	$495	$397	$2,356
Commercial	$47	$75	$508	$0	$0	$2,268	$2,898
Office	$49	$79	$535	$0	$0	$1,354	$2,017
Industrial	$28	$44	$299	$0	$0	$465	$836
Institutional	$32	$33	$226	$0	$0	$704	$995

Note:

1. Growth related capital improvement project total $17,275,000
2. City Hall expansion / renovation costs $4.0 million
3. West End Gateway costs $5.0 million.

Attachment: Preliminary Fee range estimates (5597 : DTA Developer Fee)

Table 3: Highest Cost Proposed Municipal Developer Fees

Land Use	Fire	Police	Municipal	Library	Parks	Transportation	Total
Single Family	$105	$169	$1,351	$62	$499	$995	$3,181
Multi-Family	$105	$167	$1,340	$62	$495	$442	$2,611
Commercial	$47	$75	$602	$0	$0	$2,526	$3,251
Office	$49	$79	$634	$0	$0	$1,508	$2,271
Industrial	$28	$44	$355	$0	$0	$518	$945
Institutional	$32	$33	$267	$0	$0	$784	$1,117

Note:

1. Growth related capital improvement project total $19,275,000
2. City Hall expansion / renovation costs $5.0 million
3. West End Gateway costs $6.0 million.

It is important to note that residential fees are per unit and non-residential fees are per 1,000 square feet. The conclusions presented in the tables below reflect these estimates and represent DTA's latest iteration in establishing the City's Municipal Developer Fee program. Additional detail on the fee calculations will be discussed during the next conference call. If you have any immediate questions upon review of the attached analysis, please feel free to call us at (800) 969-4382.

Attachment: Preliminary Fee range estimates (5597 : DTA Developer Fee)

dta
www.FinanceDTA.com

MEMORANDUM

March 18, 2022

To: Alissa Meeks, Special Project Manager
Charles Town, West Virginia

From: DTA

Subject: Current Preliminary Residential and Non-Residential Land Uses

DTA has updated this memorandum to present the current preliminary demographic land use projections for the City of Charles Town, West Virginia (the "City") for review by City staff. Per the March 18th discussion, population and employees are now presented in two separate columns. **Table 1** below shows the current existing residential and non-residential development as discussed in the last call with the City staff.

Table 1: Existing Development as of 2021

Land Use	Population	Employees	Units	Square Footage	Persons per Unit / Employees per 1,000 sq. ft.
Single-Family	4,800		1,631		2.94
Multi-Family	1,700		949		1.79
Commercial		2,182		1,939,237	1.13
Office		559		472,000	1.18
Industrial		411		619,787	0.66
Institutional		48		62,415	0.77

Sources:

1. Residential units and population figures for 2021 were provided by the Nielsen Company and. are consistent with the totals provided by US Census projections for 2021. Totals were further reviewed updated after consultation with the City
2. Non-residential square footage for the City was determined using the CoStar Real Estate Software Platform.
3. Persons per residential unit and employees per 1,000 square feet were determined by DTA using several sources including the Nielsen company and an employee per 1,000 square foot calculations based on factors published in the US Energy Information Administrations "Commercial Building Energy Consumption Survey" released in 2016. Totals were further reviewed and updated after consultation with the City.

Per the City staff feedback, we have reduced the current persons per household (PPH) from 2.94 to 2.52. However, given the single family total of 1631 residential units, this single family persons per household adjustment reduced the total population from 6.500 to 5,810. So, we had to adjust the multi-family persons per household upwards to 2.50 to maintain the approximate 6,500 population memo. In reviewing this, we believe the 2.52 number is too low as it makes the multi-family PPH number to high. We believe that these numbers should be adjusted to make the final land use numbers more realistic and would like the opportunity to discuss this with you.

Attachment: Memo Population 03.18.22 .v5 (5597 : DTA Developer Fee)

Table 2: Existing Development as of 2021
(Adjusted Single Family PPH from 2.94 to 2.52)

Land Use	Population	Employees	Units	Square Footage	Persons per Unit / Employees per 1,000 sq. ft.
Single-Family	4,117		1,631		2.52
Multi-Family	2,377		949		2.50
Commercial		2,182		1,939,237	1.13
Office		559		472,000	1.18
Industrial		411		619,787	0.66
Institutional		48		62,415	0.77

After you have had a chance to review this, lets set up a time to discuss. In the meantime, if you have any immediate questions upon the review of the attached analysis, please feel free to call me (800) 969-4DTA x213.

Attachment: Memo Population 03.18.22 .v5 (5597 : DTA Developer Fee)

dta
www.FinanceDTA.com

MEMORANDUM

April 18, 2022

To: Alissa Meeks, City of Charles Town WV

From: DTA Inc.

Subject: Preliminary Municipal Developer Fee Estimates.

DTA has prepared this memorandum to present the preliminary Municipal Developer Fees (the "Fees") to the City of Charles Town. (the "City"). **Table 1,** shown below, summarizes the preliminary Municipal Developer fees for six (6) fee categories. DTA has based these preliminary fee estimations on the 2021 demographic and land use numbers approved by the City staff. The fee schedule is also based on the City's Growth Related Capital Improvement Projects – Developer Fee Analysis as of November 30, 2021, as shown in **Table 2.** The conclusions presented in the table below reflect these estimates and represent DTA's latest iteration in establishing the City's Municipal Developer Fee program

Table 1: Preliminary Proposed Municipal Developer Fees

Land Use [1] [2]	Fire	Police	Municipal	Library [3]	Parks [3]	Transportation	Total
Single Family	$106	$169	$928	$62	$499	$784	$2,548
Multi-Family	$105	$167	$921	$62	$495	$349	$2,098
Commercial	$47	$75	$414	$0	$0	$1,990	$2,526
Office	$49	$79	$436	$0	$0	$1,188	$1,752
Industrial	$28	$44	$244	$0	$0	$408	$724
Institutional	$21	$33	$184	$0	$0	$618	$856

Note:

1. Residential fees are per unit and non-residential fees are per 1,000 square feet.
2. Per the City's request, a single family residence person per house hold of 2.52 was used.
3. Library and Park fees exclude non-residential development.

Table 2: Growth Related Capital Improvement Projects - Developer Fee Analysis

Facility Name	Total Cost for Facility
A. Fire Services	
Fire Services Facilities	$500,000
B. Police	
Police Facilities	$800,000
C. Municipal Facilities	
Municipal Facilities	$4,400,000
D. Library	
Library Facilities	$200,000
E. Parks	
Parks Facilities	$1,600,000
F. Transportation	
Transportation Facilities	$7,700,000
Grand Total	$15,200,000

Attachment: Charles Town Fee Memo 4.18.22 v1 with Capital project calculations (5597 : DTA Developer Fee)

Additional detail on the fee calculations will be discussed during the next conference call. If you have any immediate questions upon review of the attached analysis, please feel free to call us at (800) 969-4382.

Attachment: Charles Town Fee Memo 4.18.22 v1 with Capital project calculations (5597 : DTA Developer Fee)

DEVELOPER FEES

CITY OF CHARLES TOWN

PUBLIC FACILITIES NEEDS LIST THROUGH 20

	Facility Name	Total Cost for Facility	Off-setting Revenues	Net Cost to City
	Fire			
1	Equipment and Facility upgrade do to growth for both fire companies - Independent and Cistizens Fire Companies	**$500,000**		$ 500,000
	Fire Facilities Subtotal	**$ 500,000**	**$ -**	**$ 500,000**
	Police			
1	Vehicles and Equipment	$800,000	$ -	$ 800,000
	Offsetting Revenues			
	Police Facilities Subtotal	**$ 800,000**	**$ -**	**$ 800,000**
	Municipal Facilties			
1	Expansion of Police Headquarters - added security features and build out of existing CTUB space to accommodate larger police force	$300,000	$ -	$ 300,000
2	City Hall Expansion / Renovations - Growing community will require additional space to accommodate staff. 101 W Washington St	$3,000,000	$ -	$ 3,000,000
3	Maintenance yard and facility - new facility will be needed to house and maintain addiitonal equipment requried to serve a larger community - Water Street	$750,000	$ -	$ 750,000

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

4	Storm water equipment - Replacement street sweeper to service additionl roads / gutters resulting from growth; sweeper will preserve stormwater system by preventing debris from entering - Water Street	$350,000	$ -	$	350,000
	Offsetting Revenues				
	Municipal Facilities Subtotal	**$ 4,400,000**	**$ -**	**$**	**4,400,000**
	Library				
1	Placeholder project - Equipment to accommodate future growth	$200,000	$ -	$	200,000
	Offsetting Revenues				
	Library Facilities Subtotal	**$ 200,000**	**$ -**		**$200,000**
	Parks				
1	Expansion of Pool to accommodate growth - Jefferson Memorial Park	$700,000	$ -	$	700,000
2	Acquisition of parkland and amemities to accommodate future growth - includes tennis courts, pickle ball courts, play fields, play equipment	$500,000	$ -	$	500,000
3	Walking Bridges that connect existing parks on the west end of town. Evitts Run Park and Happy Retreat	$400,000	$ -	$	400,000
	Offsetting Revenues				
	Parks Facilities Subtotal	**$ 1,600,000**	**$ -**		**$1,600,000**
	Transportation				
1	Addition to existing bridge, new footbridge over US340 or multi-purpose path under US 340	$2,000,000	$ -	$	2,000,000

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

2	Traffic and safety enhancements at US340 and Augustine - City contribution ti improve saftey at the intersection that results fron increased traffic in the area from growth.	$1,000,000	$ -	$	1,000,000
3	Augustine Avenue Trail. Connect new development on the east side of Augustine Ave. to proposed multi-purpose trail. Includes crosswalks lighting, safety features, etc. - Location East Side Developments	$200,000	$ -	$	200,000
4	Westend Gateway, WV 51 / Summit Point road / W Washington Street - City contribution to facilitate road utility, and pedestrian improvements.	$4,000,000	$ -	$	4,000,000
5	Charles Street Improvements - N. Charles Street, Implement pan for community event space/infrastructure improvements that will enhance community engagement for new residents	$500,000	$ -	$	500,000
	Offsetting Revenues				
	Transportation Facilities Subtotal	**$ 7,700,000**		**$**	**7,700,000**
	Total	**$ 15,200,000**	**$ -**	**$**	**15,200,000**

Capital Improvement Projects per Alissa Meeks Email of 12/7/22

GROWTH RELATED CAPITAL IMPROVEMENT PR
Date: As of Novembe

Project Description	Location	Description
MUNICIPAL FACILITIES		
Expansion of police headquarters	661 S. George Street	Added security features and build CTUB space to accommodate larg

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

City Hall expansion/renovations	101 W. Washington Street	Growing community will require a accommodate staff. Could be ne likely to be retrofit of existing spa
Maintenance yard and facility	Water Street	New facility will be needed to ho additional equipment required to community.
Stormwater equipment	Water Street	Replacement street sweeper to s roads/gutters resulting from gro preserve stormwater system by p from entering.
PARKS AND RECREATION		
Expansion of pool to accommodate future growth.	Jefferson Memorial Park	Replacing pool will accommodate by expanding the pool and addin amenity will benefit new growth.
Acquisition of park land and amenities to accommodate future growth.	Various locations	Tennis courts, pickle ball courts, equipment, etc.
Walking Bridges	Evitts Run Park and Happy Retreat	Install walking bridges that conn on the west end of town.
CONNECTIVITY/TRANSPORTATION		
Feasibility study to examine options for connecting Wards 2 and 4 to downtown	- - -	RFQ pending and pricing to be d
Construction of preferred feasbility option	- - -	Could be an addition to on an ex perhaps a new footbridge over U multi-purpose path under US34

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

GROWTH RELATED CAPITAL IMPROVEMENT F
Date: As of Novemt

Project Description	Location	Description
Traffic and safety enhancements at US340 and Augustine	US340 and Augustine Avenue	City contribution to improve sa intersection that results from i the area from growth.
Augustine Avenue Trail	East side developments	Connect new developments on Augustine Avenue to proposed that has been largely funded.
Westend gateway	WV51/Summit Point Road/W. Washington Street	City contribution to facilitate rc pedestrian improvements.
Charles Street Improvements	N. Charles Street	Implement plan for community space/infrastructure improven enhance community engagem residents.
FIRE AND RESCUE		
Independent and Citizens Fire Companies	Charles Town/Ranson	Equipment and facility upgrad both fire companies.
LIBRARY		
Placeholder Project	E. Washington Street	Placeholder project pending m Library about needs resulting f

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

POLICE		
Vehicles and Equipment	661 S. George Street	Vehicles and equipment for ne resulting from growth.
MISCELLANEOUS		
Affordable housing	Various	Perhaps a new category is nee that support construction of n housing. This will be a greater new growth occurs.

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

40

Percent of Cost Allocated to New Development	Cost Allocated to New Development	Policy Background or Objective	Notes / Comments
18.97%	$94,834	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
18.97%	$151,735	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
18.97%	$56,900	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
18.97%	$569,005	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Low end estimate to renovate space to accommodate Staff. New facility could be closer to $3 to $5 million
18.97%	$142,251	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Esitmate is only for new climate controlled facility to serve growing communiy

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

18.97%	$66,384	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Estimate for equipment, Need additional research on exact sweeper needed.
19.83%	$39,665	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
19.83%	$138,828	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
19.83%	$99,163	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
19.83%	$79,330	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
17.91%	$358,114.57	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Estimate is based on the highest cost option of a footbridge.

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

17.91%	$179,057.28	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Assumes most of improvements will be covered by state and TIS contributions made by new development
17.91%	$35,811.46	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Includes crosswalkes, lighting etc.
17.91%	$716,229.13	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Existing study has costs ranging from $4 to $6 million; City assumes contribution of 20%.
17.91%	$89,528.64	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	Assumes 50% of costs due to growth and benefits for new residents.

OJECTS – DEVELOPER FEE ANALYSIS
r 30, 2021

	Estimated Costs	Notes/Comments
l out of existing ger police force.	$300,000	

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

additional space to w build but more ice.	$500,000	Low end estimate to renovate space to accommodate staff. New facility could be closer to $3 to $5 million.
use and maintain serve a larger	$750,000	Estimate is only for new, climate controlled facility to service growing community. Other upgrades to the yard are not considered growth and funded with other resources.
ervice additional wth; sweeper will preventing debris	$350,000	Estimate for equipment. Need additional research on exact sweeper needed.
existing residents g splash pad	$700,000	Estimate based on approximately 40% of design concept 2 from TTG and 100% of splash pad amenity. Another $100,000 added for partial cost (maybe 33%) to renovate pool house.
play fields, play	$500,000	How does parkland dedication ordinance impact this item?
ect existing parks	$400,000	Estimate assume 50% of project is growth related and the balance is existing.
etermined.	$75,000	Estimated cost of a feasibility study.
isting bridge;)340; or even)	$2,000,000	Estimate is based on perhaps the highest cost option of a footbridge.

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

PROJECTS - DEVELOPER FEE ANALYSIS
ber 30, 2021

	Estimated Costs	Notes/Comments
fety at the ncreased traffic in	$1,000,000	Assumes most of improvements will be covered by state and TIS contributions made by new developments.
the east side of multi-purpose trail	$200,000	Includes crosswalks, lighting, safety features, etc.
oad, utility, and	$120,000	Existing study has costs ranging from $4 to $6 million; assumes City contribution of 20%.
/ event ents that will ent for new	$500,000	Assume 50% of costs due to growth and benefits for new residents.
es due to growth for	$500,000	Waiting additional information from the fire companies on existing equipment and needs.
ore detail from rom growth.	$200,000	

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

ew sworn officers	$800,000	Assume 20 to 30 year time horizon and growth of City to 10,000 people. Estimate an additional 8 sworn officers and costs of $100,000 per officer. Pending staffing study will provide additional insight.
ded generate funds ew workforce need for the City has	TBD	Estimate TBD. Sonoma, California using impact fees to support its workforce housing needs.

Attachment: Public Facilities Needs List 2040 (5597 : DTA Developer Fee)

www.FinanceDTA.com

ASSESSMENT OF MUNICIPAL DEVELOPER FEES

CITY OF CHARLES TOWN, WV

Report Date: September 19, 2022

Public Finance
Public-Private Partnerships
Development Economics
Clean Energy Bonds

Newport Beach | San Jose | San Francisco | Riverside
Dallas | Houston | Raleigh | Tampa

www.FinanceDTA.com
614 Capital Blvd. Unit 202
Raleigh, NC 27603

CITY OF CHARLES TOWN

ASSESSMENT OF MUNICIPAL DEVELOPER FEES

Prepared for:

City of Charles Town

101 East Washington Street

Charles Town, WV 25414

Attention: Alissa Meeks, Project Manager/Parks Administrator

TABLE OF CONTENTS

SECTION		PAGE
I	EXECUTIVE SUMMARY	1
A	Organization of the Fee Study	1
B	Municipal Developer Fee Methodology and Approach	2
C	Municipal Developer Fee Schedule Summary	3
II	INTRODUCTION	5
III	LEGAL REQUIREMENTS TO JUSTIFY MUNICIPAL DEVELOPER FEES	7
A	Legal Standards Overview and History	7
IV	DEMOGRAPHICS	8
A	Existing Residential Land Uses	8
B	Existing Non-Residential Land Uses	10
C	Future Residential Land Uses (2040)	11
D	Future Non-Residential Land Uses (2040)	12
V	CAPITAL IMPROVEMENT PROJECT LIST	13
VI	METHODOLOGY USED TO CALCULATE FEES	15
A	Plan-Based Fee Methodology	15
B	Summary of Fee Methodology	15
C	Allocation of Benefits	16
VII	CALCULATION OF FEES	18
A	Fire and Rescue Fees	18
B	Police Fees	22
C	Municipal Facilities Fees – Low Capital Costs	26
D	Municipal Facilities Fees – Medium Capital Costs	30
E	Municipal Facilities Fees – High Capital Costs	34
F	Library Fees	38
G	Parks and Recreation Fees	42
H	Transportation – Low Capital Costs	46
I	Transportation – Medium Capital Costs	51

J Transportation – High Capital Costs.....56
VIII SUMMARY OF FEES.....61

APPENDICES

APPENDIX A FEE DERIVATION WORKSHEETS
APPENDIX B FACILITIES NEEDS LIST

I EXECUTIVE SUMMARY

DTA was retained by the City of Charles Town, West Virginia (the "City"), to provide a comprehensive study ("the Study") for the assessment and development of the City's Municipal Developer Fees. This study enables the City to adequately plan for new development by selecting the public facilities and costs associated with mitigating the direct and cumulative impacts of new development. The City is seeking the assessment and calculation of Municipal Developer Fees for each of the following six (6) individual categories: Fire and Rescue, Police, Municipal Facilities, Library Facilities, Parks and Recreation, and Transportation. The six fee categories will be combined into one total Municipal Developer Fee. The Municipal Developer Fee Study will recommend the appropriate fee justification methodology and fee levels to support specific types of City-selected capital facilities needed to service new growth. The purpose of this Fee Study will be to establish a nexus between anticipated development and Future Facilities for the City through 2040. Furthermore, this will ensure that all new development within the City is required to pay its "fair share" of the Future Facilities. The Municipal Developer Fees generated in this Fee Study are one-time fees typically paid prior to the issuance of a building permit and imposed on development projects by local agencies responsible for regulating land use. The fee amounts to be determined will be at levels identified as being necessary to meet the needs of new development through 2040.

A Organization of the Fee Study

This Fee Study will be presented in the following eight sections:

- Section I contains an Executive Summary and provides a brief introduction to the Fee Study and includes an overview of the proposed fees.
- Section II is an Introduction that includes a brief description of City surroundings and background information on development fee financing.
- Section III provides an overview of the legal requirements for implementing and imposing the Municipal Developer fee amounts identified in the Fee Study and satisfies the nexus requirements for each facility included as part of this Fee Study. Included is a discussion of the requirements necessary to be satisfied when establishing, increasing, or imposing a fee as a condition of new development.
- Section IV includes a discussion of land use characteristics and demand variables of projected new development such as the number of housing units and the number of non-residential building square feet, assuming current growth trends in residential and non-residential development projected through 2040.
- Section V contains the Capital Improvement Project List provided by the City.
- Section VI contains the description of the methodology used to determine the Municipal Developer Fees for Future Facilities and presents the fees for each of the land use types.

- Section VII presents the calculation of the Municipal Developer Fees for each land use.
- Section VIII presents a summary of the Municipal Developer Fees.

This Fee Study also includes an appendix section presenting the calculations and other relevant materials used to determine the findings presented in this Fee Study, as noted below:

- **Appendix A** includes the calculations used to determine the various Municipal Developer Fee levels.
- **Appendix B** includes the Facilities Needs List used to determine the various Municipal Developer Fee levels. This list is based on the Growth-Related Capital Improvement Projects – Developer Fee Analysis date as of November 30th, 2021, as provided by the City.

B Municipal Developer Fee Methodology and Approach

The methodology used to establish the Municipal Developer Fees outlined in this Study is based on a "plan," such as a Master Plan of Facilities, Capital Improvement Plan, or General Plan, which identifies a finite set of improvements to be implemented. These Facility Plans generally identify a finite set of facilities needed by the public agency and are developed according to assessments of facilities needs prepared by staff and/or outside consultants and adopted by the public agency's legislative body. Using this plan-based approach, specific costs can be projected and assigned to all land uses planned, often with a specific time period in mind that reflects new development projections.

The plan used in this Study to calculate the Municipal Developer fees is the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021. The City's Project list contains planned improvements, descriptions and estimated costs for Fire and Rescue, Police, Municipal Facilities, Library Facilities, Parks and Recreation, and Transportation projects. It's important to note that the City's Capital Improvement list presented a range of cost estimates for two of the fee sectors in this Study: the Municipal facilities sector and the Transportation sector. To account for the estimated cost ranges in these two sectors, DTA and the City determined that three (3) Municipal Developer Fee Schedules would be generated, one for each cost scenario. The fee schedules are based on the following: The Lowest Capital Cost Improvement Scenario is based on $15,275,000 of projected capital improvements, the Medium Cost Capital Improvement Scenario is based on $17,275,000 of projected capital improvements and the Highest Cost Capital Improvement Scenario is be based on $19,975,000 of projected capital improvements. These three scenarios offer the City a choice of which fee schedule to implement. The proposed Municipal Developer fee summary presenting these Capital Cost Improvement scenarios is presented in **Table ES-1** on the following page.

Table ES-1: Proposed Municipal Developer Fee Summary
Three Proposed Capital Cost Improvement Scenarios [1]

`Facility Name	Total Cost for Facility (Lowest) [2]	Total Cost for Facility (Medium) [2]	Total Cost for Facility (Highest) [2]
A. Fire and Rescue			
Fire and Rescue Services Facilities	$500,000	$500,000	$500,000
B. Police			
Police Facilities	$800,000	$800,000	$800,000
C. Municipal Facilities			
Municipal Facilities	$4,400,000	$5,400,000	$6,400,000
D. Library Facilities			
Library Facilities	$200,000	$200,000	$200,000
E. Parks and Recreation			
Parks and Recreation Facilities	$1,600,000	$1,600,000	$1,600,000
F. Transportation			
Transportation Facilities	$7,775,000	$8,775,000	$9,775,000
Total	$15,275,000	$17,275,000	$19,275,000

Notes:

1. Facilities Costs are based on the City's Growth-Related Capital Improvement Projects – Developer Fee Analysis as of November 30, 2021.
2. Lowest, Medium, and Highest refer to the three Capital Improvement Cost Scenarios.
3. Municipal Facilities and Transportation Facilities costs are different in each Scenario.

C Municipal Developer Fee Schedule Summary

Per the results of this Study, the total Municipal Developer fee amounts required to support new development's share of Future Facilities are identified in **Tables ES-2, ES-3 and ES-4** and presented below. Fees presented for each scenario in this Fee Study reflect the Municipal Developer fees that may be imposed on new development in the City. Residential fees are listed as per unit and non-residential fees are per 1,000 square feet. The cost estimates for Future Facilities used in this section are in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News-Record ("ENR") and/or an annual adjustment based upon current West Virginia law.

Table ES-2: Proposed Municipal Developer Fee Schedule
Lowest Cost Capital Improvement Scenario [2]

Land Use [1]	Fire and Rescue	Police	Municipal Facilities	Library Facilities	Parks and Recreation	Transportation	Total
Single-Family	$126	$201	$1,107	$62	$499	$792	$2,787
Multi-Family	$125	$200	$1,098	$62	$495	$352	$2,331
Commercial	$28	$45	$247	$0	$0	$2,010	$2,329
Office	$30	$47	$260	$0	$0	$1,200	$1,536
Industrial	$17	$26	$145	$0	$0	$412	$600
Institutional	$19	$31	$169	$0	$0	$624	$842

Notes:

1. Residential fees are per unit and non-residential fees are per 1,000 square feet.
2. Fees based on Total Capital Improvements $15,275,000.

Table ES-3: Proposed Municipal Developer Fee Schedule
Medium Cost Capital Improvement Scenario[2]

Land Use [1]	Fire and Rescue	Police	Municipal Facilities	Library Facilities	Parks and Recreation	Transportation	Total
Single-Family	$126	$201	$1,359	$62	$499	$894	$3,140
Multi-Family	$125	$200	$1,348	$62	$495	$397	$2,626
Commercial	$28	$45	$303	$0	$0	$2,268	$2,644
Office	$30	$47	$319	$0	$0	$1,354	$1,749
Industrial	$17	$26	$178	$0	$0	$465	$686
Institutional	$19	$31	$207	$0	$0	$704	$961

Notes:

1. Residential fees are per unit and non-residential fees are per 1,000 square feet.
2. Fees based on Total Capital Improvements $17,275,000.

Table ES-4: Proposed Municipal Developer Fee Schedule
Highest Cost Capital Improvement Scenario[2]

Land Use [1]	Fire and Rescue	Police	Municipal Facilities	Library Facilities	Parks and Recreation	Transportation	Total
Single-Family	$126	$201	$1,610	$62	$499	$995	$3,494
Multi-Family	$125	$200	$1,597	$62	$495	$442	$2,921
Commercial	$28	$45	$359	$0	$0	$2,526	$2,958
Office	$30	$47	$378	$0	$0	$1,508	$1,963
Industrial	$17	$26	$211	$0	$0	$518	$772
Institutional	$19	$31	$245	$0	$0	$784	$1,079

Notes:

1. Residential fees are per unit and non-residential fees are per 1,000 square feet.
2. Fees based on Total Capital Improvements $19,275,000.

II INTRODUCTION

Founded in 1786, the City of Charles Town ("the City") is located along the Eastern Panhandle of West Virginia. Located in Jefferson County, just inside the eastern gateway of West Virginia, it is approximately an hour's drive to the greater Baltimore/Washington, D.C. metropolitan area. Due to this this proximity and the availability of commuter train service, Charles Town is considered an attractive home for commuters in the region. The City covers approximately 5.81 square miles and is home to over 6,500 people. Surrounded by the hills of the Blue Ridge mountains, nearby cities include Harpers Ferry, Ranson, and Martinsburg West Virginia, and Winchester Virginia.

In order to adequately plan for new development and identify the public facilities and costs associated with mitigating the direct and cumulative impacts of new development, DTA was retained by the City to provide a comprehensive study ("the Study") for the assessment and development of the City's Municipal Developer Fees. The City is seeking the assessment and calculation of Municipal Developer Fees for each of the following six (6) individual categories: Fire and Rescue, Police, Municipal Facilities, Library Facilities, Parks and Recreation, and Transportation. The six fee categories are to be combined into one total Municipal Developer Fee. The Municipal Developer Fee Study will recommend the appropriate fee justification methodology and fee levels to support specific types as City-selected capital facilities needed to service new growth. Furthermore, the purpose of this Fee Study will be to establish a nexus between the anticipated development and Future Facilities for the City through 2040 and to ensure that all new development within the City is required to pay its "fair share" of the Future Facilities. The Municipal Developer Fees generated in this Fee Study are one-time fees typically paid prior to the issuance of a building permit and imposed on development projects by local agencies responsible for regulating land use.

The fee amounts to be determined will be at levels identified as being necessary to meet the needs of projected new development through 2040.

Fees are calculated to fund the cost of facilities needed to meet the needs of new development. **Many of the calculations and totals presented in the tables of this Study are factored out to several decimal places and may not sum due to rounding. In the interest of clarity, they will be noted with footnotes where necessary.** The steps followed in the Fee Study include:

1. **Demographic Assumptions**: Identify future growth that represents the increased demand for Future Facilities;
2. **Facility Needs and Costs**: Determine the number of public facilities required to support new development and the costs of such facilities;
3. **Cost Allocation**: Allocate costs per equivalent dwelling unit or equivalent benefit unit; and

4. **Fee Schedule**: Calculate the Municipal Developer Fee amount per residential unit and per 1,000 square feet for non-residential development.

III LEGAL REQUIREMENTS TO JUSTIFY MUNICIPAL DEVELOPER FEES

A Legal Standards Overview and History

The levy of Municipal Developer Fees is one authorized method of financing the public facilities necessary to mitigate the impacts of new development. One-time fees paid by all new development to help pay for the infrastructure needed by that new development. Fees are typically paid by developers, builders, or other property owners that are seeking to develop property. In this manner, developers, and property owners pay their "fair share" of needed capital facilities. A Municipal Developer fee may be levied for each type of capital improvement required for new development, with the payment of the fee typically occurring prior to the beginning of construction of a dwelling unit or non-residential building. Fees are often levied at final map recordation, upon the issuance of a Certificate of Occupancy, or more commonly, at building permit issuance.

The Municipal Developer Fees presented in this Study are not considered Development Impact Fees under West Virginia Code Section 70-20-1 *et seq.*, which provides that municipalities (and also counties) have only such powers as (i) are expressly granted to them by the Constitution or legislature, (ii) are necessarily or fairly implied in or incident to the powers expressly granted, and (iii) essential to its decaled objects and purposes. Article 20 of Chapter 7 applies only to counties and all the provisions authorizing impact fees are limited to counties.

Development within the city limits is still subject to the County's Impact fee, as the County's Impact fee is composed of several components dedicated to Schools, Law Enforcement, Parks and Recreation, and Emergency Medical Services ("EMS"). All of those components apply to residential construction in the City except the law enforcement as the City has its own police department. Similarly, only the law enforcement and EMS component would apply to the commercial/industrial projects in the City.

IV DEMOGRAPHICS

To determine the facilities needed to serve new development and establish fee amounts to fund such facilities, the City has provided DTA with material containing information of future residential information and land use development within the City through 2040. For the purpose of this Fee Study, DTA categorized developable residential land uses as single-family and multi-family residences. Developable non-residential land uses within the City's commercial and industrial zones are categorized as commercial, office, industrial and institutional and are summarized in detail in the following section.

DTA relied on the following sources to estimate the number of housing units and non-residential building square feet to be built within the City: the 2040 Charles Town Comprehensive Plan, the City's 2014 Transportation Study, the US Census Bureau and the Nielsen Company Demographics and Land Uses Services. Additionally, DTA relied on the CoStar Real Estate Manager Software Platform ("CoStar") to estimate the existing non-residential development within the City.

Future residents and employees are expected to create additional demand for facilities that existing development facilities cannot adequately service. In order to accommodate new development in an orderly manner, while maintaining the current quality of life in the City, the facilities on the City's current Facilities Inventory and Facilities Needs List (Section V) need to be constructed.

For those facilities that are needed to mitigate demand from new development, facility costs have been allocated to only new development. In those instances when it has been determined that the new facilities will serve both existing and new development, facility costs have been allocated based on proportionate benefit [see the Equivalent Dwelling Unit ("EDU") and Equivalent Benefit Unit ("EBU") discussion in Section VI.]

In addition, DTA has determined that utilizing a Persons Served population, comprised of all residents and 50% of employees is common practice in quantifying the impact of a new development in a given service area and this metric will be used in both residential and non-residential employee population and calculations throughout this report.

A Existing Residential Land Uses

Demographic data provided by the Nielsen Company, a leading information, measurement, and data analytics company, was used to estimate the existing number of housing units and population in the City. These figures are generally confirmed by the U.S. Census Bureau and the City of Charles Town.

Table 1 presented below provides a summary of the land uses covered in this fee study. As indicated, the study will provide Development Developer Fees for six (6) specific land use categories; single-family, multi-family, commercial, office, industrial, and institutional. The table provided below is meant to provide an example of typical land uses found in each category and is not intended to be a comprehensive list of all the City's potential land uses.

Table 1: Summary of Land Use Categories

Land Use	Definition
Single-Family Residential	Includes single-family detached homes.
Multi-Family Residential	Includes buildings with attached residential units including apartments, town homes, condominiums, and all other non-mobile home units not classified as a Detached Dwelling residential unit that may be subject to this fee in accordance with state law.
Commercial	Includes but is not limited to buildings used as the following: ▪ Restaurants, bars, drive-thru fast-food establishments; ▪ Pharmacy, grocery stores, auto centers, office supply stores; ▪ Department/specialty stores, variety stores, liquor stores; ▪ Service Stations, hair salons, home improvement stores; and ▪ Convenience retail, hotels/motels, discount stores.
Office	Includes but is not limited to office buildings used as the following: ▪ General office buildings, medica/dental offices, office parks.
Industrial	Includes but is not limited to industrial buildings used as the following: ▪ General Industrial, warehouse/distribution, light manufacturing; and ▪ Truck terminals, freight delivery, logistics wholesaling.
Institutional	Includes but is not limited to buildings used as the following: ▪ Professional urgent care and private hospitals, rehabilitation centers; ▪ Assisted living, nursing, and memory care facilities.

Notably, DTA attempted to utilize metrics (e.g., average household size, square footage, etc.) that standardized existing demographics with DTA's projections.

Using the demographic information attained from the City's General Plan Housing Element, the Nielsen Company, and other sources such as the US Census Bureau, DTA has assigned a City resident-per-unit factor of 2.52 for single-family residential units and 2.50 for multi-family residential units. These totals were reviewed with city staff and incorporated into the Study.

The persons per unit figures presented were used by DTA to determine the single-family and multi-family populations. According to the information provided by the Nielsen Company, a leading information, data and market measurement firm there are currently 1,631 single-family units and 949 multi-family units respectively, within the City. Using the 2.52 and 2.50 residents per unit figures, DTA has determined that there are 4,117 existing single-family residents and 2,377 multi-family residents. Combined, the current City population is comprised of 6,494 current residents living in 2,580 single-family and multi-family homes. **Table 2** below summarizes the existing demographics for the residential land uses.

Table 2: Estimated Existing Residential Development [1]

Residential Land Use	Existing Residents	Existing Housing Units [2]	Residents per Unit
Single-Family	4,117	1,631	2.52
Multi-Family	2,377	949	2.50
Total	**6,494**	**2,580**	

Notes:

1 Numbers may not sum due to rounding (1,631 x 2.52 = 4,117)
2 Housing Unit numbers per the Nielsen Company.

B Existing Non-Residential Land Uses

According to information provided by CoStar, a leading real estate database, information, and analytics software platform, there are also approximately 3.09 million total square feet of existing non-residential development in the City; including approximately 1.90 million square feet of existing commercial development, 472 thousand square feet of existing office space, 619 thousand square feet of industrial development and 62 thousand square feet of institutional development.

In order to calculate how many employees that the City has in these categories, DTA utilized an employee's-per-thousand-square-foot factor ("EPSF") of 1.13 for the commercial sector, 1.18 for the office sector, 0.66 for the industrial sector and 0.77 for the institutional sector. For example, for commercial land uses DTA calculated an EPSF of 1.13, i.e., on average there are 1.13 employees per thousand square feet of industrial development. The numbers are estimates determined by DTA based on the employee's-per-thousand-square-foot factors published in the U.S. Energy Information Administration's "Commercial Buildings Energy Consumption Survey" ("CBECS") released in December of 2016. Due to the comprehensive nature of this type of survey, it takes several years to update the numbers.

As indicated, the 3.09 million square feet of existing non-residential development is based on information provided by both the City and DTA's research using CoStar, the Nielsen Company, and other data sources. Using these figures and standard employment generation rates for commercial, office, industrial, and institutional square footage, DTA has estimated the potential employee capacity for non-residential development available in the City.

These calculations resulted in 2,182 existing commercial employees, 559 office employees, 411 existing industrial employees and 48 institutional employees within the city. Note that the actual total employee figures for non-residential development will likely vary somewhat from DTA estimates because of vacancies, property utilizations, etc. However, for purposes of the fee calculation, the City is interested in the total number of employees that could be generated by the identified square footage for a particular land use. The same method is applied to future non-residential space and associated employee estimates.

For many of the facilities considered in this Fee Study, EDUs will be used to allocate benefits among fee categories. EDU calculations are based on the number of residents and employees ("Persons Served") generated by each land use class (EDUs are covered in more detail in the following sections). Based on years of performing a variety of fiscal and economic impact studies and with experience in a variety of both public and private sectors, DTA has determined that utilizing a service population, or Persons Served population, comprised of all residents and 50% of employees is common fiscal practice in quantifying the impact of a new development in each service area. This is presented in **Table 3** below.

Table 3: Estimated Existing Non-Residential Development

Non-Residential Land Use	Existing Employees	Persons Served	Existing Building Square Feet
Commercial	2,182	1,091	1,939,237
Office	559	280	472,000
Industrial	411	206	619,787
Institutional	48	24	62,415
Total	**3,200**	**1,600**	**3,093,439**

C Future Residential Land Uses (2040)

Population projects were generated using the growth experienced from 2010 to 2021 and projecting it out to 2040. Using this information, the City is expected to grow by 1,607 residents by the end of the build-out period. Maintaining the City resident-per-unit factor of 2.52 for single-family residences and 2.50 for multi-family residences, these totals project that 403 single-family housing units and 235 multi-family housing units, totaling 638 units will be built in the City through 2040, the time horizon utilized for this Fee Study. **Table 4** presented below summarizes the projected number of housing units for residential land uses over the build-out period.

Table 4: Future Residential Development [1]

Residential Land Use	Future Residents	Future Housing Units	Residents per Unit
Single-Family	1,019	403	2.52
Multi-Family	588	235	2.50
Total	**1,607**	**638**	

Note:

1 Numbers may not sum due to rounding.

D Future Non-Residential Land Uses (2040)

In terms of future non-residential property, the City expects the development of over 643 thousand square feet over the build-out period. This includes over 403 thousand square feet of commercial development, 98 thousand square feet of office, 128 thousand square feet of industrial and 13 thousand square feet of non-residential development. To generate the 2040 non-residential build-out square footage totals presented in this Fee Study, DTA used a normalized growth rate of 1.0% for each of the non-residential sectors.

Table 5: Future Non-Residential Development

Non-Residential Land Use	Future Employees	Persons Served	Future Building Square Feet
Commercial	454	227	403,573
Office	116	58	98,227
Industrial	86	43	128,983
Institutional	10	5	12,989
Total	**666**	**333**	**643,772**

In addition, as indicated above, using the same methodology presented in the previous section, and to determine the number of employees in each of these categories, DTA has maintained the same EPSF factor each of the non-residential land uses over the build-out period. Through 2040, these calculations result in 454 future commercial employees, 116 future office employees 86 future industrial employees and 10 future institutional employees within the City.

V CAPITAL IMPROVEMENT PROJECT LIST

Identification of the facilities to be financed is a critical component of any plan-based Municipal Developer Fee program. In the broadest sense, the purpose of the fees is to protect the public health, safety, and general welfare by providing for adequate public facilities. Identification of the facilities may be included in an applicable General or Specific Plan, other public documents, or by reference to a Capital Improvement Program ("CIP").

The City has provided DTA with the list of Future Facilities to be included in the Fee Study (the "Facilities Needs List"). These planned facilities come from the Growth-Related Capital Improvement Projects – Developer Fee Analysis as of November 30, 2021. For the purposes of the City's fee program, the Facilities Needs List is intended to be the official public document identifying the facilities eligible to be financed, in whole or in part, through the levy of a Municipal Developer Fee on new development within the City. The Facilities Needs List is organized by facility element (or type) and includes a cost section consisting of six rows, which are presented and defined in **Table 6** below.

Table 6: Explanation of Cost Section

Column Title	Contents	Source
Total Cost for Facility	The total estimated facility cost, including engineering, design, construction, land acquisition, and equipment (as applicable).	City
Offsetting Revenues to New and Existing Development [1]	Share of total offsetting revenues allocated to new and existing development.	City
Net Cost to City	The difference between the total cost and the offsetting revenues (column 1 plus column 2).	Calculated by DTA
Percent of Cost Allocated to New Development	Net cost allocated to new development based on new development's share of facilities.	Calculated by DTA and the City
Net Cost Allocated to New Development	The net cost to the City multiplied by the percentage cost allocated to new development.	Calculated by DTA
Policy Background or Objective	Identifies the policy source or rationale for facility need.	City Capital Improvement Projects

Note:

1 Offsetting Revenues are included in developer municipal fee calculations, in the case of Charles Town, WV, Offsetting Revenues total zero.

The City's Capital Improvement Project list contains planned improvements, descriptions and estimated costs for Fire and Rescue, Police, Municipal Facilities, Library Facilities, Parks and Recreation, and Transportation projects. It's important to note that the City's Capital Improvement list presented a range of cost estimates for two of the fee sectors in this Study: the Municipal facilities sector and Transportation sector. To account for the estimated cost ranges in these two sectors, DTA and the City determined that three (3) Municipal Developer Fee Schedules would be generated, one for each cost scenario. They are as follows: The Lowest Capital Cost Improvement Scenario is based on $15,275,000 of projected capital improvements, the Medium Cost Capital Improvement Scenario is based on $17,275,000 of projected capital improvements and the Highest Cost Capital Improvement Scenario is based on $19,975,000 of projected capital improvements. These three scenarios offer the City a choice of which fee schedule to implement. The proposed Municipal Developer fee summary presenting these Capital Cost Improvement scenarios is presented in **Table 7** below. (The detailed Facilities Needs List is presented in full in **Appendix B** at the end of this Fee Study).

Table 7: Summary Capital Improvement Project List [1]
Three Proposed Capital Cost Improvement Scenarios

Facility Name	Total Cost for Facility (Lowest) [2]	Total Cost for Facility (Medium) [2]	Total Cost for Facility (Highest) [2]
A. Fire and Rescue			
Fire and Rescue Services Facilities	$500,000	$500,000	$500,000
B. Police			
Police Facilities	$800,000	$800,000	$800,000
C. Municipal Facilities			
Municipal Facilities	$4,400,000	$5,400,000	$6,400,000
D. Library Facilities			
Library Facilities	$200,000	$200,000	$200,000
E. Parks and Recreation			
Parks and Recreation Facilities	$1,600,000	$1,600,000	$1,600,000
F. Transportation			
Transportation Facilities	$7,775,000	$8,775,000	$9,775,000
Total	$15,275,000	$17,275,000	$19,275,000

Notes:

1. Facilities costs based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021.
2. Lowest, Medium, and Highest refer to the three Capital Improvement Scenarios.
3. Municipal Facilities and Transportation Facilities costs are different in each scenario.

VI METHODOLOGY USED TO CALCULATE FEES

There are many methods of calculating fees, but they are all based on determining the cost of needed improvements and assigning those costs equitably to various types of development. In determining a reasonable nexus for each specific type of public facility, DTA utilized the Plan – Based fee methodology described below, based upon the data and information available from the City and its current infrastructure policies.

A Plan-Based Fee Methodology

The methodology used to establish the Municipal Developer Fees outlined in this Study is based on a "plan," such as a Master Plan of Facilities, Capital Improvement Plan, or General Plan, which identifies a finite set of improvements to be implemented. These Facility Plans generally identify a finite set of facilities needed by the public agency and are developed according to assessments of facilities needs prepared by staff and/or outside consultants and adopted by the public agency's legislative body. Using this plan-based approach, specific costs can be projected and assigned to all land uses planned, often with a specific time period in mind that reflects new development projections. By using population, units, and residential and non-residential square footage numbers, it is possible to assign a cost allocation percentage for both new and existing development. In preparing a Municipal Developer fee analysis, facilities costs attributed to future development can then be allocated to each land use class in proportion to the demand caused by each type of development.

B Summary of Fee Methodology

In this Fee Study, the Plan-based methodology is used to generate Municipal Developer fees for Fire and Rescue, Police, Municipal Facilities, Library Facilities, Parks and Recreation, and Transportation. This is summarized in **Table 8** below.

Table 8: Methodology (by Fee Category Type)

Fee Category	Methodology [1]	Basis of Methodology
Fire and Rescue	Plan-Based Fee	Facilities Needs List
Police	Plan-Based Fee	Facilities Needs List
Municipal Facilities	Plan-Based Fee	Facilities Needs List
Library Facilities	Plan-Based Fee	Facilities Needs List
Parks and Recreation	Plan-Based Fee	Facilities Needs List
Transportation	Plan-Based Fee	Facilities Needs List

Note:

1 There are a number of acceptable methodologies used in these fee studies; plan-based, capacity based, level of service, buy-in, etc. This table is included to let the reader know that the methodology used in this Study is one of many available choices and as a reference for future updates.

C Allocation of Benefits

C.1 Equivalent Dwelling Units ("EDUs") and Equivalent Benefit Units ("EBUs")

The methodologies employed in this Fee Study use Equivalent Dwelling Units ("EDUs") and Equivalent Benefit Units ("EBUs") as the method of identifying and quantifying benefit of certain facilities and ensuring that an equitable portion of the total facilities costs are allocated to future growth, based on the proportion of need generated by that growth. Specifically, EDUs are generated in the demographic portion of this Fee Study and are used to generate the land use calculations. EDUs are a means of quantifying different land uses in terms of their equivalence to a residential dwelling unit, where equivalence is measured in terms of potential infrastructure use or benefit for each type of public facility. In this Study, EDUs are used as a basis of allocation for Fire and Rescue, Police, Library Facilities, and Parks and Recreation. In contrast, the service factor for Transportation facilities are based on trip ends, so EBUs are used to allocate costs to future growth and generate fees. The factor utilized to determine the EBUs for each of the six (6) land types in this sector are Peak Hour Trips ("PHTs"). This is explained further later in this section and in detail in **Appendix A**.

Table 9: Basis of Allocation by Fee Category Type

Land Use	Basis of Allocation of Benefit (EDU/EBU Factor)	Total EDUs/EBUs
Fire and Rescue	Persons Served	3,975
Police	Persons Served	3,975
Municipal Facilities	Persons Served	3,975
Library Facilities	Persons Served	3,209
Parks and Recreation	Persons Served	3,209
Transportation	PM Peak Hour Trips	9,721

As shown in **Table 9** above, throughout this Study, Fire and Rescue, Police and Municipal Facilities will total 3,975 EDUs as these sectors generate fees for both residential and non-residential development. Library Facilities and Parks and Recreation will generate a total of 3,209 EDUs because these sectors generate fees for only residential development. The Transportation Sector will generate 9,721 EBUs because this sector generates fees using trips instead or persons serviced.

C.2 Persons Served

For many of the facilities considered in this Fee Study, service population (or Persons Served) will be used to allocate benefits among fee categories. For purposes of this Fee Study, the Persons Served calculations are based on the number of residents per dwelling unit (i.e., persons per household) and number of employees per 1,000 sq. ft. generated by each land use class. Based on years of performing a variety of fiscal

and economic impact studies and with experience in a variety of both public and private sectors, DTA has determined that utilizing a service population, or Persons Served population, comprised of all residents and 50% of employees is common fiscal practice in quantifying the impact of a new development in each service area. This number suggests that a resident generally has twice the fiscal impact of an employee.

C.3 PM Peak Hour Trips ("PHT"s)

Transportation Impact Fees were calculated for each of the six (6) land use categories based on the number of PM Peak Hour Trips ("PHTs") generated by each land use. Peak Hour Trips are published by the Institute of Transportation Engineers ("ITE") Publication Trips Generation, 10th Edition. These PM Peak hour Trips define daily trip generation per dwelling unit (for residential units) and daily trip generation per 1,000 building square feet of each category of non-residential development. Per the ITE, a trip or trip end is a single or one-direction person or vehicle movement with either the origin or the destination existing or entering) inside a Study Site. In technical terms, a trip has an origin and a destination at its respective ends (known as trip ends). Each trip end is part of a trip. For trip site generation, the focus is the trips entering and existing a single site. Specifically Peak hour trips are total vehicular trips entering and leaving a development project during the period between 4:00 pm and 6:00 pm which experiences the highest sum of traffic volumes entering or leaving the development. The PM peak hour measurement was used over other measurements such as average trip rates or weekend trips rates because transportation analyses are based on congestion, which is largely a result of more people trying to use the transportation system during the busiest hours, and it is usually the period for which road improvements were designed.

The following sections present the reasonable relationship of benefit, impact, and proportionality tests for each fee element (i.e., Fire and Rescue, Police, Municipal Facilities, Library Facilities, Parks and Recreation, and Transportation and the analysis undertaken to apportion costs for each type of facility. Detailed fee calculation worksheets for each type of facility are included in **Appendix A**.

VII CALCULATION OF FEES

A Fire and Rescue Fees

A.1 Fire and Rescue Facilities

The Fire and Rescue element includes those facilities required within the City to maintain adequate fire protection services. The purpose of this updated section is to address the fire protection demands City-wide, including areas that are currently experiencing (or are planned for) growth and/or are areas that exceed the desired response emergency services response times. Particular focus will be on the identification of Fire Department Facilities, including training facilities, fire apparatuses, vehicles, and fire equipment due to new development in all areas of the City.

In order to serve new development through build-out, the City identified the need for an equipment and facilities upgrade for both fire companies – Independent and Citizens Fire Companies.

Table 10: Purposed of Fire and Rescue Facilities Municipal Developer Fee

Identify the Purpose of the Fee	Fire and Rescue Facilities
Identify the use of the fee.	Equipment and Facility upgrade due to growth for both fire companies - Independent and Citizens Fire Companies
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development will generate additional residents and employees who will require additional service calls, thereby increasing the need for trained fire protection personnel. Equipment and vehicles used to provide these services will have to be purchased or replaced and facilities will need to be constructed to meet this increased demand. Thus, a reasonable relationship exists between the need for Fire Services Facilities and impact of residential and non-residential development. The Municipal Developer fees collected from new development will be used exclusively for Fire protection purposes.

Equipment used to provide these services will have to be purchased or replaced and facilities will need to be constructed to meet this increased demand. Thus, a reasonable relationship exists between the need for fire services facilities and impact of residential and non-residential development. The Fire and Rescue Municipal Developer fees collected from new development will be used exclusively for fire protection purposes. The fee would be collected as the development occurs (usually at the building permit stage).

As the new development occurs, the impact is generated. All new development within the City, irrespective of location, contributes to the direct and cumulative impacts of development on fire department facilities and creates the need for new facilities to accommodate growth. Without future development, many of the facilities on the Facilities Needs Lists would not be necessary. For certain other facilities, the costs have been allocated to both existing and new development based on their level of benefit. For the reasons presented herein, there is a reasonable relationship between the need for the fire department facilities included on the Facilities Needs List and all new development within the City.

Table 11 presented below identifies the proposed facilities and equipment acquisition costs to be funded in whole or in part with the fees collected for Fire and Rescue Facilities.

Table 11: Fire and Rescue Facilities Costs

Fire Department Facilities	Facility Cost
Equipment Facilities Upgrade	$500,000
Fire and Rescue Facilities Subtotal	**$500,000**
Offsetting Revenues	-
Fire and Rescue Facilities Total	**$500,000**

A.2 Calculation Methodology

The cost estimates for the Fire and Rescue category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021. The fees have been calculated for both residential and non-residential development. According to the City, it has been determined that these facilities are needed to serve new development. Currently, these facilities are generally operating at an appropriate and acceptable level of service. Therefore, the costs of facilities have been allocated to both new development and existing development based on their expected usage at build-out.

Consequently, given the information provided by the City, DTA has determined that 80.67% of the remaining costs will be allocated to existing development and must be funded by other means such as taxes, grants, bonds, other fees, etc. while 19.33% of the costs will be allocated to new development.

As illustrated in **Appendix A** at the end of this Fee Study, the total number of EDUs calculated for both residential and non-residential development equals 3,975 (total EDUs), with 3,206 (existing EDUs) assigned to existing development and 768 (new EDUs) assigned to new development.

As indicated in Section VI, Fire and Rescue, Police and Municipal Facilities will all total 3,975 EDUs as these sectors generate fees for both residential and non-residential development. Library Facilities and Parks and Recreation will generate a total of

3,209 EDUs because these sectors generate fees for only residential development. The Transportation Sector will generate 9,721 EBUs because this sector uses trips instead or persons served.

In order to calculate the facility cost allocation percentage of new development shown in the table below, the number of EDUs assigned to new development is divided by the overall total number of EDUs and illustrated with the following equation: new EDUs/total EDUs = 19.33%.

As illustrated below in **Table 12**, 19.33% of the $500,000 in total facilities costs equals $96,652 in new development costs. So, in total, $96,652 out of $500,000 in Fire and Rescue Department costs would be covered by Municipal Developer fees on new development.

Table 12: Fire and Rescue Facilities Cost Allocation Summary [1]

Development Type	Percentage Allocated to New Development	Facility Cost Allocation
Existing Development	80.67%	$403,348
New Development	19.33%	$96,652
Total	100.00%	$500,000

Note:

1. May not sum due to rounding.

A.3 Fee Calculation

The fee amounts required by each land use type to finance new development on the Fire and Rescue Facilities Needs List are presented in the following table. The single-family and multi-family residential fees are calculated per housing unit and the commercial, office, industrial, and institutional development fees are calculated per 1,000 square feet. All of the calculations are based on costs per EDUs generated by dividing the cost to new development of $96,652 by the number of new EDUs (768), resulting in a $126 cost per EDU.

As shown in **Table 13**, the Municipal Developer Fee is $126 per unit for a single-family residence and is the same as the cost per EDU (a ratio of 1:1). Since a multi-family unit generates approximately 0.99 EDUs, the fee for a multi-family residence is determined by the cost allocation per unit, i.e., 0.99 times the single-family fee or $125 per unit.

Similarly, the proposed non-residential fees are equal to the cost allocation by square footage for each land use category. The commercial sector generates approximately 0.22 EDUs. Thus, the fee for commercial development is based on the cost allocation per unit, i.e., 0.22 times the single-family fee or $28 per 1,000 square feet. This can be seen at the bottom of the next page in **Table 14**.

Table 13: Fire and Rescue Facilities Fee Derivation

Land Use Type	Municipal Developer Fee per Unit	Municipal Developer Fee per 1,000 Square Feet	Fire Department Facilities Costs Financed by Fees
Single-Family Residential	$126		$50,759
Multi-Family Residential	$125		$29,300
Commercial		$28	$11,314
Office		$30	$2,899
Industrial		$17	$2,131
Institutional		$19	$249
		Developer Fee Cost Total	**$96,652**
		Costs Allocated to Sources other than Developer Fees	$403,348
		Total Fire Department Facilities Costs	**$500,000**

The same methodology (0.23 EDUs times the single-family fee of $126) is used to calculate a fee of $30 per 1,000 square feet for office development and for calculating the fee of $17 per 1,000 square foot for industrial development and $19 per 1,000 square foot for institutional development.

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News Record ("ENR").

Table 14: Proposed Fire and Rescue Facilities Fee Summary [1]

Land Use Type	EDUs	Fee Per Unit (1,000 Sq. Ft.)
Single-Family Residential	1.00	$126
Multi-Family Residential	0.99	$125
Commercial	0.22	$28
Office	0.23	$30
Industrial	0.13	$17
Institutional	0.15	$19

Note:

1 May not sum due to rounding.

B Police Fees

B.1 Police Facilities

The Police Facilities element includes those facilities used by the City Police Department to maintain police services. To serve new development through the year 2040, the City Police Department has identified the need for additional vehicles and equipment. The facilities, equipment, and vehicles used to provide these services will have to be purchased or replaced to meet this increased demand. Thus, a reasonable relationship exists between the need for Law Enforcement Facilities and impact of residential and non-residential development.

The Police Facilities fees collected from new development will be used exclusively for Police Department purposes. All new development within the City, regardless of location, contributes to the direct and cumulative impacts of development on Police Department facilities and creates the need for new facilities to accommodate growth. Without future development, many of the facilities on the Facilities Needs Lists would not be necessary. For certain other facilities, the costs have been allocated to both existing and new development based on their level of benefit. For the reasons presented herein, there is a reasonable relationship between the need for the Police facilities included on the Facilities Needs List and all new development within the City.

Table 15: Purposed of Police Facilities Municipal Developer Fee

Identify the Purpose of the Fee	Police Facilities
Identify the use of the fee.	Vehicle and Equipment replacement to accommodate new development.
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development will generate additional residents and employees who will require additional service calls, thereby increasing the need for trained Police Department personnel. Equipment and vehicles used to provide these services will have to be purchased or replaced to meet this increased demand. Thus, a reasonable relationship exists between the need for Police Facilities and impact of residential and non-residential development. The Municipal Developer fees collected from new development will be used exclusively for Law Enforcement purposes.

Table 16 below identifies the proposed facilities and equipment to be funded in whole or in part with the fees collected for Law Enforcement improvements. All facilities costs are based on estimates provided by the City and are part of the City's effort to maintain and improve the City's Law Enforcement Facilities.

B.2 Calculation Methodology

The cost estimates for the Police Facilities category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021 and is calculated for both residential and non-residential development. According to the City, it has been determined that these facilities are needed to serve new development. Currently, these facilities are generally operating at an appropriate and acceptable level of Law Enforcement service. Therefore, as shown below, the costs of facilities have been allocated to new development and existing development based on their expected usage at build-out.

Table 16: Police Facilities Costs

Police Department Facilities	Facility Cost
Vehicles and Equipment	$800,000
Police Facilities Subtotal	**$800,000**
Offsetting Revenues	-
Police Facilities Total	**$800,000**

Given the information provided by the City Police Department and using the plan-based approach, DTA has determined that 80.67% of the costs will be allocated to existing development and must be funded by other means such as taxes, grants, bonds, other fees, etc. while 19.33% of the costs will be allocated to new development.

As illustrated in **Appendix A** at the end of this Fee Study, the total number of EDUs calculated for both residential and non-residential development equals 3,975 (total EDUs), with 3,206 (existing EDUs) assigned to existing development and 768 (new EDUs) assigned to new development.

In order to calculate the facility cost allocation percentage of new development shown in the table below, the number of EDUs assigned to new development is divided by the overall total number of EDUs and illustrated with the following equation: new EDUs/total EDUs = 19.33%.

As illustrated in **Table 17** below, 19.33% of the $800,000 in total facilities costs equals $154,643 in new development costs. So, in total, $154,643 out of $800,000 in Police Facilities costs would be covered by Municipal Developer fees on new development.

Table 17: Police Facilities Cost Allocation Summary [1]

Development Type	Percentage Allocated to New Development	Facility Cost Allocation
Existing Development	80.67%	$645,357
New Development	19.33%	$154,643
Total	**100.00%**	**$800,000**

Note:

1. May not sum due to rounding.

B.3 Fee Calculation

The fee amounts required by each land use type to finance new development on the Facilities Needs List are presented on the following page. The single-family and multi-family residential fees are calculated per housing unit and the commercial, office, industrial and institutional development fees are calculated per 1,000 square feet. All the calculations are based on costs per EDUs generated by dividing the cost to new development of $154,643 by the number of new EDUs (768), resulting in a $201 cost per EDU.

As shown on the following page in **Table 18**, the Police Municipal Developer Fee is $201 per unit for a single-family residence and is the same as the cost per EDU (a ratio of 1:1). Since a multi-family unit generates approximately 0.99 EDUs, the fee for a multi-family residence is given by the cost allocation per unit, i.e., 0.99 times the single-family fee or $200 per unit.

Similarly, the proposed non-residential fees are equal to the cost allocation by square footage for each land use category. This is shown at the bottom of the next page in **Table 19**. The commercial sector generates approximately 0.22 EDUs. Thus, the fee for commercial development is determined by the cost allocation per unit, i.e., 0.22 times the single-family fee or $45 per 1,000 square feet.

The same methodology (0.23 EDUs times the single-family fee) is used to calculate a fee of $47 per 1,000 square feet for office development and a fee of $26 per 1,000 square foot for industrial development and $31 per square foot for institutional development.

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News Record ("ENR").

Table 18: Police Facilities Fee Derivation

Land Use Type	Municipal Developer Fee per Unit	Municipal Developer Fee per 1,000 Square Feet	Law Enforcement Facilities Costs Financed by Fees
Single-Family Residential	$201		$81,214
Multi-Family Residential	$200		$46,880
Commercial		$45	$18,103
Office		$47	$4,638
Industrial		$26	$3,410
Institutional		$31	$398
		Developer Fee Cost Total	**$154,643**
		Costs Allocated to Sources Other than Developer Fees	$645,357
		Total Police Facilities Costs	**$800,000**

Table 19: Proposed Police Facilities Fee Summary

Land Use Type	EDUs	Fee Per Unit (1,000 Sq. Ft.)
Single-Family Residential	1.00	$201
Multi-Family Residential	0.99	$200
Commercial	0.22	$45
Office	0.23	$47
Industrial	0.13	$26
Institutional	0.15	$31

C Municipal Facilities Fees – Low Capital Costs

C.1 Municipal Facilities

The Municipal Facilities element includes the facilities necessary to provide basic governmental services and public facilities maintenance services throughout the City. The proposed Municipal Developer Fee discussed in this section, if adopted, would be imposed, collected, and spent on the necessary acquisition of land, construction of new public buildings, and expansion of existing City facilities to accommodate new growth, specifically the facilities identified on the Facilities Needs List.

In order to serve future development through General Plan build-out, the City has identified the need for a City Hall expansion, an expansion of Police headquarters, a Maintenance yard and facility, and Storm Water equipment. Specifically, the fee will be used to pay for the Municipal Facilities Department projects (or portions of the projects) identified below in **Table 20** and in detail in **Appendix B**. The fees cannot be used for any other purpose.

Table 20: Purposed of Municipal Facilities Developer Fee (Low)

Identify the Purpose of the Fee	Municipal Facilities
Identify the use of the fee.	This includes the expansion of City facilities, maintenance yards and storm water equipment
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development in the City will generate additional residents and employees who will increase the demand for Citywide services and general government functions. Population and growth have a direct impact on the need for government services and facilities. Thus, a reasonable relationship exists between new development and government facilities, which will have to be acquired to meet the increased demand. Fees collected from new development will be used exclusively for Municipal Facilities on the Facilities Needs List.

Table 21 presented on the following page identifies all the proposed facilities and land to be funded in whole or in part with the fees collected for Municipal Facilities improvements. All facilities cost estimates are based on Growth-Related Capital Improvements Projects list provided by the City and are part of the City's effort to maintain and improve the City's Municipal Facilities.

C.2 Calculation Methodology

The cost estimates for the Municipal Facilities category were provided by the City and fees are calculated for both residential and non-residential development. Each land use classification was assigned an EDU factor that was derived from the number of Persons Served, which is defined as the persons per household (for residential units) and 50% of the number of employees per 1,000 building square feet of each category of non-residential development.

Projected new development in the City will generate additional residents and employees who will increase the demand for City-wide services and general government functions. Each development will contribute to the need for new Municipal Facilities. Without future development (both residential and non-residential), the City would have no need to construct many of the public facilities on the Facilities Needs List. For all other facilities, the costs have been allocated to both existing and new development based on their level of benefit.

Consequently, all new development within the City, irrespective of location, contributes to the direct and cumulative impacts of development on public facilities and creates the need for new facilities to accommodate growth. Using the plan-based approach introduced earlier, the Municipal Facilities Fee was calculated for both residential and non-residential land uses as detailed below in **Table 21** and in **Appendix A**.

Table 21: Municipal Facilities Costs (Low)

Municipal Facilities – Low Capital Costs	Facility Cost
Expansion of Police Headquarters	$300,000
City Hall Expansion	$3,000,000
Maintenance Yard and Facility	$750,000
Storm Water Equipment	$350,000
Municipal Facilities Subtotal	**$4,400,000**
Offsetting Revenues	-
Municipal Facilities Total	**$4,400,000**

The cost estimates for the Municipal Facilities category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021. The fees are calculated for both residential and non-residential development. According to the City, it has been determined that these facilities are needed to serve new development. Currently, these facilities are generally operating at an appropriate and acceptable level of service. Therefore, the costs of facilities have been allocated to new development and existing development based on their expected usage at build-out.

As illustrated in **Appendix A** at the end of this Study, the total number of EDUs calculated for both residential and non-residential development equals 3,975 (total EDUs), with 3,206 (existing EDUs) assigned to existing development and 768 (new EDUs) assigned to new development. In order to calculate the facility cost allocation percentage of new development shown in the table below, the number of EDUs assigned to new development is divided by the overall total number of EDUs and illustrated with the following equation: new EDUs/total EDUs = 19.33%. (Again, the mathematics behind this calculation is presented in detail in Appendix A.)

As shown below in **Table 22**, given the information provided by the City and using the plan-based approach referred to earlier, DTA has determined that 80.67% of the costs of the new facilities will be allocated to existing development and must be funded by other means such as taxes, grants, bonds, other fees, etc. while 19.33% of the costs will be allocated to new development.

Table 22: Municipal Facilities Cost Allocation Summary (Low) [1]

Development Type	Percentage Allocated to New Development	Facility Cost Allocation
Existing Development	80.67%	$3,549,462
New Development	19.33%	$850,538
Total	**100.00%**	**$4,400,000**

Note:

1. May not sum due to rounding.

As illustrated above, 19.33% of the $4,400,000 in total facilities costs equals $850,538 in new development costs. In total, $850,538 out of $4,400,000 in Municipal Facilities costs would be covered by Municipal Developer Fees on new development.

C.3 Fee Calculation

The fee amounts required by each land use type to finance new development on the Facilities Needs List are presented on the following page. The single-family and multi-family residential fees are calculated per housing unit and the office, commercial, industrial, and institutional development fees are calculated per 1,000 square feet. All of the calculations are based on costs per EDUs generated by dividing the cost to new development of $850,538 by the number of new EDUs (768), resulting in a $1,107 cost per EDU.

As shown on **Table 23 below,** the Municipal Facilities Developer Fee is $1,107 per unit for a single-family residence and is the same as the cost per EDU (a ratio of 1:1). Since a multi-family unit generates approximately 0.99 EDUs, the fee for a multi-family residence is based on the cost allocation per unit, i.e., 0.99 times the single-family fee or $1,098 per unit.

Table 23: Municipal Facilities Fee Derivation (Low)

Land Use Type	Municipal Developer Fee per Unit	Municipal Developer Fee per 1,000 Square Feet	Municipal Facilities Costs Financed by Fees
Single-Family Residential	$1,107		$446,679
Multi-Family Residential	$1,098		$257,842
Commercial		$247	$99,566
Office		$260	$25,507
Industrial		$145	$18,754
Institutional		$169	$2,190
		Developer Fee Total	**$850,538**
		Costs Allocated to Sources Other than Developer Fees	$3,549,462
		Total Municipal Facilities Costs	**$4,400,000**

Similarly, the proposed non-residential fees are equal to the cost allocation by square footage for each land use category. The commercial sector generates approximately 0.22 EDUs. Thus, the fee for commercial development is based on the cost allocation per unit, i.e., 0.22 times the single-family fee or $247 per 1,000 square feet. This is seen below in **Table 24**.

The same methodology (0.23 EDUs times the single-family fee) is used to calculate a fee of $260 per 1,000 square feet of office development. The remaining non-residential fees are calculated using the same methodology. This is presented in detail in **Appendix A** at the end of the Study. A summary of proposed fees is presented below.

Table 24: Proposed Municipal Facilities Fee Summary (Low)

Land Use Type	EDUs	Fee Per Unit (1,000 Sq. Ft.)
Single-Family Residential	1.00	$1,107
Multi-Family Residential	0.99	$1,098
Commercial	0.22	$247
Office	0.23	$260
Industrial	0.13	$145
Institutional	0.15	$169

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News Record ("ENR").

D Municipal Facilities Fees – Medium Capital Costs

D.1 Municipal Facilities

The Municipal Facilities element includes the facilities necessary to provide basic governmental services and public facilities maintenance services throughout the City. The proposed Municipal Developer Fee discussed in this section, if adopted, would be imposed, collected, and spent on the necessary acquisition of land, construction of new public buildings, and expansion of existing City facilities to accommodate new growth, specifically the facilities identified on the Facilities Needs List.

In order to serve future development through General Plan build-out, the City has identified the need for a City Hall expansion, an expansion of Police headquarters, a Maintenance yard and facility, and Storm Water equipment. Specifically, the fee will be used to pay for the Municipal Facilities Department projects (or portions of the projects) identified below in **Table 25** and in detail in **Appendix B**. The fees cannot be used for any other purpose.

Table 25: Purpose of Municipal Facilities Developer Fee (Medium)

Identify the Purpose of the Fee	Municipal Facilities
Identify the use of the fee.	This includes the expansion of City facilities, maintenance yards and storm water equipment
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development in the City will generate additional residents and employees who will increase the demand for Citywide services and general government functions. Population and growth have a direct impact on the need for government services and facilities. Thus, a reasonable relationship exists between new development and government facilities, which will have to be acquired to meet the increased demand. Fees collected from new development will be used exclusively for Municipal Facilities on the Facilities Needs List.

Table 26 presented on the following page identifies all the proposed facilities and land to be funded in whole or in part with the fees collected for Municipal Facilities improvements. All facilities cost estimates are based on Growth-Related Capital Improvements Projects list provided by the City and are part of the City's effort to maintain and improve the City's Municipal Facilities.

D.2 Calculation Methodology

The cost estimates for the Municipal Facilities category were provided by the City and fees are calculated for both residential and non-residential development. Each land use classification was assigned an EDU factor that was derived from the number of Persons Served, which is defined as the persons per household (for residential units) and 50% of the number of employees per 1,000 building square feet of each category of non-residential development.

Projected new development in the City will generate additional residents and employees who will increase the demand for City-wide services and general government functions. Each development will contribute to the need for new Municipal Facilities. Without future development (both residential and non-residential), the City would have no need to construct many of the public facilities on the Facilities Needs List. For all other facilities, the costs have been allocated to both existing and new development based on their level of benefit.

Consequently, all new development within the City, irrespective of location, contributes to the direct and cumulative impacts of development on public facilities and creates the need for new facilities to accommodate growth. Using the plan-based approach introduced earlier, the Municipal Facilities Fee was calculated for both residential and non-residential land uses as detailed below in **Table 26** and in **Appendix A**.

Table 26: Municipal Facilities Costs (Medium)

Municipal Facilities – Medium Capital Costs	Facility Cost
Expansion of Police Headquarters	$300,000
City Hall Expansion	$5,000,000
Maintenance Yard and Facility	$750,000
Storm Water Equipment	$350,000
Municipal Facilities Subtotal	**$5,400,000**
Offsetting Revenues	-
Municipal Facilities Total	**$5,400,000**

The cost estimates for the Municipal Facilities category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021. The fees are calculated for both residential and non-residential development. According to the City, it has been determined that these facilities are needed to serve new development. Currently, these facilities are generally operating at an appropriate and acceptable level of service. Therefore, the costs of facilities have been allocated to new development and existing development based on their expected usage at build-out.

As illustrated in **Appendix A** at the end of this Fee Study, the total number of EDUs calculated for both residential and non-residential development equals 3,975 (total EDUs), with 3,206 (existing EDUs) assigned to existing development and 768 (new EDUs) assigned to new development. In order to calculate the facility cost allocation percentage of new development shown in the table below, the number of EDUs assigned to new development is divided by the overall total number of EDUs and illustrated with the following equation: new EDUs/total EDUs = 19.33%. (Again, the mathematics behind this calculation is presented in detail in Appendix A.)

As shown below in **Table 27**, given the information provided by the City and using the plan-based approach referred to earlier, DTA has determined that 80.67% of the costs of the new facilities will be allocated to existing development and must be funded by other means such as taxes, grants, bonds, other fees, etc. while 19.33% of the costs will be allocated to new development.

Table 27: Municipal Facilities Cost Allocation Summary (Medium) [1]

Development Type	Percentage Allocated to New Development	Facility Cost Allocation
Existing Development	80.67%	$4,356,158
New Development	19.33%	$1,043,842
Total	**100.00%**	**$5,400,000**

Note:

1. May not sum due to rounding.

As illustrated above, 19.33% of the $5,400,000 in total facilities costs equals $1,043,842 in new development costs. In total, $1,043,842 out of $5,400,000 in Municipal Facilities costs would be covered by Municipal Developer Fees on new development.

D.3 Fee Calculation

The fee amounts required by each land use type to finance new development on the Facilities Needs List are presented on the following page. The single-family and multi-family residential fees are calculated per housing unit and the office, commercial, industrial, and institutional development fees are calculated per 1,000 square feet. All of the calculations are based on costs per EDUs generated by dividing the cost to new development of $1,043,842 by the number of new EDUs (768), resulting in a $1,359 cost per EDU.

As shown on **Table 28,** the Municipal Developer Fee is $1,359 per unit for a single-family residence and is the same as the cost per EDU (a ratio of 1:1). Since a multi-family unit generates approximately 0.99 EDUs, the fee for a multi-family residence is based on the cost allocation per unit, i.e., 0.99 times the single-family fee or $1,348 per unit.

Table 28: Municipal Facilities Fee Derivation (Medium)

Land Use Type	Municipal Developer Fee per Unit	Municipal Developer Fee per 1,000 Square Feet	Municipal Facilities Costs Financed by Fees
Single-Family Residential	$1,359		$548,196
Multi-Family Residential	$1,348		$316,442
Commercial		$303	$122,194
Office		$319	$31,305
Industrial		$178	$23,016
Institutional		$207	$2,688
		Developer Fee Total	**$1,043,842**
		Costs Allocated to Sources Other than Developer Fees	$4,356,158
		Total Municipal Facilities Costs	**$5,400,000**

Similarly, the proposed non-residential fees are equal to the cost allocation by square footage for each land use category. The commercial sector generates approximately 0.22 EDUs. Thus, the fee for commercial development is based on the cost allocation per unit, i.e., 0.22 times the single-family fee or $303 per 1,000 square feet as seen below in **Table 29**.

The same methodology (0.23 EDUs times the single-family fee) is used to calculate a fee of $319 per 1,000 square feet of office development. The remaining non-residential fees are calculated using the same methodology. This is presented in detail in **Appendix A** at the end of the Study. A summary of proposed fees is presented below.

Table 29: Proposed Municipal Facilities Fee Summary (Medium)

Land Use Type	EDUs	Fee Per Unit (1,000 Sq. Ft.)
Single-Family Residential	1.00	$1,359
Multi-Family Residential	0.99	$1,348
Commercial	0.22	$303
Office	0.23	$319
Industrial	0.13	$178
Institutional	0.15	$207

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News Record ("ENR").

E Municipal Facilities Fees – High Capital Costs

E.1 Municipal Facilities

The Municipal Facilities element includes the facilities necessary to provide basic governmental services and public facilities maintenance services throughout the City. The proposed Municipal Developer Fee discussed in this section, if adopted, would be imposed, collected, and spent on the necessary acquisition of land, construction of new public buildings, and expansion of existing City facilities to accommodate new growth, specifically the facilities identified on the Facilities Needs List.

In order to serve future development through General Plan build-out, the City has identified the need for a City Hall expansion, an expansion of Police headquarters, a Maintenance yard and facility, and Storm Water equipment. Specifically, the fee will be used to pay for the Municipal Facilities Department projects (or portions of the projects) identified below in **Table 30** and in detail in **Appendix B**. The fees cannot be used for any other purpose.

Table 30: Purposed of Municipal Facilities Developer Fee (High)

Identify the Purpose of the Fee	Municipal Facilities
Identify the use of the fee.	This includes the expansion of City facilities, maintenance yards and storm water equipment
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development in the City will generate additional residents and employees who will increase the demand for Citywide services and general government functions. Population and growth have a direct impact on the need for government services and facilities. Thus, a reasonable relationship exists between new development and government facilities, which will have to be acquired to meet the increased demand. Fees collected from new development will be used exclusively for Municipal Facilities on the Facilities Needs List.

Table 31 presented on the following page identifies all the proposed facilities and land to be funded in whole or in part with the fees collected for Municipal Facilities improvements. All facilities cost estimates are based on Growth-Related Capital Improvements Projects list provided by the City and are part of the City's effort to maintain and improve the City's Municipal Facilities.

E.2 Calculation Methodology

The cost estimates for the Municipal Facilities category were provided by the City and fees are calculated for both residential and non-residential development. Each land use classification was assigned an EDU factor that was derived from the number of Persons Served, which is defined as the persons per household (for residential units) and 50% of the number of employees per 1,000 building square feet of each category of non-residential development.

Projected new development in the City will generate additional residents and employees who will increase the demand for City-wide services and general government functions. Each development will contribute to the need for new Municipal Facilities. Without future development (both residential and non-residential), the City would have no need to construct many of the public facilities on the Facilities Needs List. For all other facilities, the costs have been allocated to both existing and new development based on their level of benefit.

Consequently, all new development within the City, irrespective of location, contributes to the direct and cumulative impacts of development on public facilities and creates the need for new facilities to accommodate growth. Using the plan-based approach introduced earlier, the Municipal Facilities Fee was calculated for both residential and non-residential land uses as detailed below in **Table 31** and in **Appendix A**.

Table 31: Municipal Facilities Costs (High)

Municipal Facilities - High Capital Costs	Facility Cost
Expansion of Police Headquarters	$300,000
City Hall Expansion	$5,000,000
Maintenance Yard and Facility	$750,000
Storm Water Equipment	$350,000
Municipal Facilities Subtotal	**$6,400,000**
Offsetting Revenues	-
Municipal Facilities Total	**$6,400,000**

The cost estimates for the Municipal Facilities category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021. The fees are calculated for both residential and non-residential development. According to the City, it has been determined that these facilities are needed to serve new development. Currently, these facilities are generally operating at an appropriate and acceptable level of service. Therefore, the costs of facilities have been allocated to new development and existing development based on their expected usage at build-out.

As illustrated in **Appendix A** at the end of this Fee Study, the total number of EDUs calculated for both residential and non-residential development equals 3,975 (total EDUs), with 3,206 (existing EDUs) assigned to existing development and 768 (new EDUs) assigned to new development. In order to calculate the facility cost allocation percentage of new development shown in the table below, the number of EDUs assigned to new development is divided by the overall total number of EDUs and illustrated with the following equation: new EDUs/total EDUs = 19.33%. (Again, the mathematics behind this calculation is presented in detail in Appendix A.)

As shown below in **Table 32**, given the information provided by the City and using the plan-based approach referred to earlier, DTA has determined that 80.67% of the costs of the new facilities will be allocated to existing development and must be funded by other means such as taxes, grants, bonds, other fees, etc., while 19.33% of the costs will be allocated to new development.

Table 32: Municipal Facilities Cost Allocation Summary (High) [1]

Development Type	Percentage Allocated to New Development	Facility Cost Allocation
Existing Development	80.67%	$5,162,854
New Development	19.33%	$1,237,146
Total	**100.00%**	**$6,400,000**

Note:

1. May not sum due to rounding.

As illustrated above, 19.33% of the $6,400,000 in total facilities costs equals $1,237,146 in new development costs. In total, $1,237,146 out of $6,400,000 in Municipal Facilities costs would be covered by Municipal Developer Fees on new development.

E.3 Fee Calculation

The fee amounts required by each land use type to finance new development on the Facilities Needs List are presented on the following page. The single-family and multi-family residential fees are calculated per housing unit and the office, commercial, industrial, and institutional development fees are calculated per 1,000 square feet. All of the calculations are based on costs per EDUs generated by dividing the cost to new development of $1,237,146 by the number of new EDUs (768), resulting in a $1,610 cost per EDU.

As shown on **Table 33** below, the Municipal Developer Fee is $1,610 per unit for a single-family residence and is the same as the cost per EDU (a ratio of 1:1). Since a multi-family unit generates approximately 0.99 EDUs, the fee for a multi-family residence is based on the cost allocation per unit, i.e., 0.99 times the single-family fee or $1,597 per unit.

Table 33: Municipal Facilities Fee Derivation (High)

Land Use Type	Municipal Developer Fee per Unit	Municipal Developer Fee per 1,000 Square Feet	Municipal Facilities Costs Financed by Fees
Single-Family Residential	$1,610		$649,714
Multi-Family Residential	$1,597		$375,042
Commercial		$359	$144,823
Office		$378	$37,102
Industrial		$211	$27,279
Institutional		$245	$3,186
		Developer Fee Total	**$1,237,146**
		Costs Allocated to Sources Other than Developer Fees	$5,162,854
		Total Municipal Facilities Costs	**$6,400,000**

Similarly, the proposed non-residential fees are equal to the cost allocation by square footage for each land use category. The commercial sector generates approximately 0.22 EDUs. Thus, the fee for commercial development is based on the cost allocation per unit, i.e., 0.22 times the single-family fee or $359 per 1,000 square feet. This is shown below in **Table 34**.

The same methodology (0.23 EDUs times the single-family fee) is used to calculate a fee of $378 per 1,000 square feet of office development. The remaining non-residential fees are calculated using the same methodology. This is presented in detail in **Appendix A** at the end of the Study. A summary of proposed fees is presented below.

Table 34: Proposed Municipal Facilities Fee Summary (High)

Land Use Type	EDU	Fee Per Unit (1,000 Sq. Ft.)
Single-Family Residential	1.00	$1,610
Multi-Family Residential	0.99	$1,597
Commercial	0.22	$359
Office	0.23	$378
Industrial	0.13	$211
Institutional	0.15	$245

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News Record ("ENR").

F Library Fees

F.1 Library Facilities

The Library Faculties element includes the facilities necessary to provide basic services throughout the City. The proposed fees discussed in this section, if adopted, would be imposed, collected, and spent on equipment to accommodate new growth, specifically the facilities identified on the Facilities Needs List. Typical library equipment includes books and material, computer equipment, required replacement of facilities and capital improvements.

Specifically, the fee will be used to pay for the Library Facilities projects (or portions of the projects) identified below and in **Appendix A**. The fees cannot be used for any other purpose.

Table 35: Purpose of Library Facilities Municipal Developer Fee

Identify the Purpose of the Fee	Library Facilities
Identify the use of the fee.	This includes equipment to accommodate future growth.
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential development in the City will generate additional residents who will increase the demand for Citywide services and general government functions. Population and growth have a direct impact on the need for Library services. Thus, a reasonable relationship exists between new development and Library Facilities, which will have to be acquired to meet the increased demand. Fees collected from new development will be used exclusively for Library Facilities on the Facilities Needs List.

Table 36 presented on the following page identifies all the proposed facilities and land to be funded in whole or in part with the fees collected for Library Facilities improvements. All facilities costs are based on estimates provided by the City and are part of the City's effort to maintain and improve the City's Library Facilities.

F.2 Calculation Methodology

The cost estimates for the Library Facilities category were provided by the City and fees are calculated for residential development. Each land use classification was assigned an EDU factor that was derived from the number of Persons Served, which is defined as the persons per household (for residential units). In contrast with the fee sections discussed earlier, library fees exclude non-residential development.

New development in the City will generate additional residents and employees who will increase the demand for City-wide services and Library functions. Each development will contribute to the need for new Library Facilities. Without future development, the City would have no need to construct many of the library facilities on the Facilities Needs List. For all other facilities, the costs have been allocated to both existing and new development based on their level of benefit.

Consequently, all new development within the City, irrespective of location, contributes to the direct and cumulative impacts of development on public facilities and creates the need for new facilities to accommodate growth. Using the plan-based approach introduced earlier, the Library Facilities Fee was calculated exclusively for residential land uses as detailed in **Appendix A**. Non-residential development is excluded from fee calculations in this section.

Table 36: Library Facilities Costs

Library Facilities	Facility Cost
Equipment to Accommodate Future Growth	$200,000
Library Facilities Subtotal	**$200,000**
Offsetting Revenues	-
Library Facilities Total	**$200,000**

The cost estimates for the Library Facilities category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021. The fees are calculated for both residential and non-residential development. According to the City, it has been determined that these facilities are needed to serve new development. Currently, these facilities are generally operating at an appropriate and acceptable level of service. Therefore, the costs of facilities have been allocated to new development and existing development based on their expected usage at build-out.

Consequently, given the information provided by the City and using the plan-based approach referred to earlier, DTA has determined that 80.17% of the costs will be allocated to existing development and must be funded by other means such as taxes, grants, bonds, other fees, etc., while 19.83% of the costs will be allocated to new development.

As illustrated in **Appendix A** at the end of this Fee Study, the total number of EDUs

calculated for residential development equals 3,209 (total EDUs), with 2,572 (existing EDUs) assigned to existing development and 636 (new EDUs) assigned to new development.

In order to calculate the facility cost allocation percentage of new development shown in the table below, the number of EDUs assigned to new development is divided by the overall total number of EDUs and illustrated with the following equation: new EDUs/total EDUs = 19.83%.

As illustrated below, 19.83% of the $200,000 in total facilities costs equals $39,665 in new development costs. In total, $39,665 out of $200,000 in Library Facilities costs would be covered by Municipal Developer fees on new development.

Table 37: Library Facilities Cost Allocation Summary [1]

Development Type	Percentage Allocated to New Development	Facility Cost Allocation
Existing Development	80.17%	$160,335
New Development	19.83%	$39,665
Total	**100.00%**	**$200,000**

Note:

1. May not sum due to rounding.

F.3 Fee Calculation

The fee amounts required by each land use type to finance new development on the Facilities Needs List are presented on the following page. The single-family and multi-family residential fees are calculated per housing unit. All of the calculations are based on costs per EDUs generated by dividing the cost to new development of $39,665 by the number of new EDUs (636), resulting in a $62.30 cost per EDU.

As shown in **Table 38** below, the Library Facilities Municipal Developer fee is $62.30 per unit for a single-family residence and is the same as the cost per EDU (a ratio of 1:1). Since a multi-family unit generates approximately 0.99 EDUs, the fee for a multi-family residence is based on the cost allocation per unit, i.e., 099 times the single-family fee or $61.80 per unit. Unlike the fees previously discussed in this Study, Library Facilities Fees only apply to residential development, non-residential development is excluded.

Table 38: Library Facilities Fee Derivation

Land Use Type	Municipal Developer Fee Per Unit	General Services Costs Financed by Fees
Single-Family Residential	$62.30	$25,148
Multi-Family Residential	$61.80	$14,517
Developer Fee Total		**$39,665**
Costs Allocated to Sources Other than Developer Fees		$160,335
Total Library Facilities Costs		**$200,000**

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News Record ("ENR").

Table 39: Library Facilities Fee Summary

Land Use Type	EDUs	Fee Per Unit
Single-Family Residential	1.00	$62.30
Multi-Family Residential	0.99	$61.80

G Parks and Recreation Fees

G.1 Parks and Recreation Facilities

The Parks and Recreation Development element will serve the City Parks by providing facilities for recreation while enhancing the community's appeal and quality of life. The type of facilities described in this section are illustrated in **Table 40** and include pool facility expansion, acquisition of parkland and amenities and walking bridges. The Fee Study includes a component for the development of new park and recreation facilities to serve new residential development for the City through 2040.

In addition to improving the overall quality of life for residents, excellent park and recreation programs are important for the well-being of a city's residential and non-residential community. Not only do parks make the community more attractive to residents (providing a stronger market base for local businesses), but parks can also directly influence a city's ability to enhance its fiscal base by attracting commercial and industrial businesses.

Table 40: Purpose of Parks and Recreation Municipal Developer Fee

Identify the Purpose of the Fee	Parks and Recreation Development Facilities
Identify the use of the fee.	The expansion of pool facilities, recreational facilities, acquisition of parkland and amenities and walking bridges.
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential development will generate an increased demand for Park Development Facilities. Population and growth will have a direct impact on the need for Park Development Facilities. New development and the consequential increase in demand will necessitate the improvement/expansion of existing Park and Recreation Development Facilities. Fees collected from new development will be used exclusively for the improvement of Community Park Development Facilities on the Facilities Needs List.

Table 41 presented below identifies the proposed facilities and improvement costs to be funded in whole or in part with the fees collected for Park Development Facilities. The cost estimates for the Park Development category were provided by the City and based on the City's Growth-Related Capital Improvements Projects-Developer Fee Analysis as of November 30, 2021.

Table 41: Park and Recreation Development Facilities Costs

Parks and Recreation Development Facilities	Facility Cost
Expansion of Pool	$700,000
Acquisition of Parkland and Amenities	$500,000
Walking Bridges	$400,000
Parks and Recreation Development Facilities Subtotal	**$1,600,000**
Offsetting Revenues	-
Parks and Recreation Development Facilities Total	**$1,600,000**

G.2 Calculation Methodology

The fee amount for Parks and Recreation Development Facilities is calculated for both new and existing development using the plan-based approach discussed throughout this Fee Study. However, unlike the other Municipal Developer Fees discussed in the Fee Study, parks fees are generated exclusively from residential development. Non-residential development is excluded from fee calculations in this section.

In order to accurately calculate the Parks and Recreation Development fees, DTA employed the plan-based approach for each of the three proposed park facilities on the Facilities Needs List on an individual basis and then aggregated the totals to determine the final Municipal Developer Fee. Fee calculations for each individual facility listed are presented in **Appendix A**.

Consequently, given the information provided by the City, DTA has determined that 80.17% of the remaining costs will be allocated to existing development and must be funded by other means such as taxes, grants, bonds, other fees, etc., while 19.83% of the costs will be allocated to new development.

As illustrated in **Appendix A** at the end of this Fee Study, the total number of EDUs calculated for residential development equals 3,209 (total EDUs), with 2,572 (existing EDUs) assigned to existing development and 636 (new EDUs) assigned to new development.

In order to calculate the facility cost allocation percentage of new development shown in the table below, the number of EDUs assigned to new development is divided by the overall total number of EDUs and illustrated with the following equation: new EDUs/total EDUs = 19.83%.

As illustrated below in **Table 42**, 19.83% of the $1,600,000 in total facilities costs equals $317,321 in new development costs. So, in total, $317,321 out of $1,600,000 in Parks and Recreation Development costs would be covered by Municipal Developer fees on new development.

Table 42: Parks and Recreation Development Facilities Cost Allocation Summary [1]

Development Type	Percentage Allocated to New Development	Facility Cost Allocation
Existing Development	80.17%	$1,282,679
New Development	19.83%	$317,321
Total	**100.00%**	**$1,600,000**

Note:

1. May not sum due to rounding.

G.3 Fee Calculation

The fee amounts required by each land use type to finance new development on the Parks and Recreation Development Facilities Needs List are presented in the table below. Both the single-family and multi-family residential fees are calculated per housing unit. All the calculations are based on costs per EDUs generated by dividing the cost to new development of $317,321 by the number of new EDUs (636), resulting in a $499 cost per EDU.

As shown in **Table 43** below, the building Municipal Developer Fee is $499 per unit for a single-family residence and is the same as the cost per EDU (a ratio of 1:1). Since a multi-family unit generates approximately 0.99 EDUs, the fee for a multi-family residence is determined by the cost allocation per unit, i.e., 0.99 times the single-family fee or $495 per unit.

Table 43: Parks and Recreation Development Facilities Fee Derivation

Land Use Type	Municipal Developer Fee per Unit	Parks and Recreation Development Facilities Costs Financed by Fees
Single-Family Residential	$499	$201,187
Multi-Family Residential	$495	$116,134
	Developer Fee Total	**$317,321**
	Costs Allocated to Sources Other than Developer Fees	$1,282,679
	Total Parks and Recreation Facilities Costs	**$1,600,000**

Table 44 below shows the generated Municipal Developer Fees for Parks and Recreation.

Table 44: Parks and Recreation Development Facilities Fee Summary

Land Use Type	EDUs	Fee Per Unit
Single-Family Residential	1.00	$499
Multi-Family Residential	0.99	$495

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News Record ("ENR").

H Transportation – Low Capital Costs

H.1 Transportation Facilities

The City's goal is to improve the City's Transportation Facilities over a period of approximately 20-years. Improvements focus on new bridges and additions to existing bridges, traffic and safety enhancements, improvements in safety at intersections, crosswalks, lighting, pedestrian improvements, and additional infrastructure. This additional infrastructure support is necessary to provide safe and efficient vehicular access throughout the City. The proposed Municipal Developers Fee is to help meet the transportation demand of new development through 2040. The City identified the need for the transportation infrastructure and equipment, as shown below in **Table 45**.

The Municipal Developer Fee will provide a source of revenue to the City to allow for the acquisition, installation, and construction of needed Transportation facilities, which in turn will both preserve the quality of life in the City and protect the health, safety, and welfare of the existing and future residents and employees. Transportation Fees will be calculated using the Plan-based approach discussed in Section VI.

Table 45: Purpose of Transportation Municipal Developer Fee (Low)

Identify the Purpose of the Fee	Transportation Facilities
Identify of the use of the fee.	Various roadway improvements including, but not limited to, crosswalks, lighting, bridges, and road pedestrian safety.
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development will generate additional residents and employees who will create additional vehicular and non-vehicular traffic within the City limits. Streets will have to be improved or extended to meet the increased demand and to efficiently direct increased traffic flow. Thus, there is a relationship between new development and the need for new transportation facilities. Municipal Developer Fees collected from new development will be used exclusively for Traffic Facilities on the Needs List.

Identification of the facilities to be financed is a critical component of any Municipal Developer fee program. In the broadest sense, the purpose of Developer Fees is to protect the public health, safety, and general welfare by providing for Transportation facilities. The City has provided DTA with the list of Future Facilities (the "Facilities Needs List") to be included in the Fee Study. For the purposes of the City's Municipal program, the Facilities Needs List is intended to be the official public document

identifying the facilities eligible to be financed, in whole or in part, through the levy of a Municipal Developer fee on new development within the City. The Facilities Needs List is organized by facility element (or type) and includes cost information, as outlined in **Table 46** below.

The facilities included are provided by the City and reflect either the City's goals of maintaining and improving a specific area, or they are part of a more formal policy document, such as a General Plan, Capital Improvement Plan, etc. Specific estimated facility costs are provided by the City and used as a basis for determining the allocation of revenues between new and existing development.

The table below outlines the proposed facilities and respective costs along with any offsetting revenues. A list of Transportation facilities is included below and in **Appendix B** at the end of this Study. The cost estimates for the Transportation category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021.

Table 46: Transportation Facilities Costs (Low)

Transportation Facilities – Low Capital Costs	Facility Costs
Transportation Feasibility Study	$75,000
Additions to Existing Bridge and New Bridge	$2,000,000
Traffic Safety Enhancements at US340 and Augustine	$1,000,000
Augustine Ave. Trail	$200,000
Westend Gateway, WV 51/Summit Point Rd./W Washington St.	$4,000,000
Charles Street Improvements	$500,000
Transportation Facilities Subtotal	**$7,775,000**
Offsetting Revenue	$0.00
Transportation Facilities Total	**$7,775,000**

Transportation Developer Fees were calculated for each of the six (6) land use categories and are based on the number of PM Peak Hour Trips (PHTs) generated by each land use. As indicated earlier in Section VI, Peak Hour Trips are total vehicular trips entering and leaving a development project during the period between 4:00 pm and 6:00 pm which is the timeframe that experiences the highest sum of traffic volumes entering or leaving the development. Total PHTs were calculated by applying these trips rates to the various dwelling unit counts and non-residential square feet identified in the demographics section of this Fee Study. As discussed in Section VI, the Institute of Transportation Engineers (ITE) uses PM peak hours to define daily trip generation per dwelling unit (for residential units) and daily trip generation per 1,000 building square feet of each category of non-residential development.

All proposed Transportation facilities were sized to meet the needs of both existing and future residents and employees. Therefore, the costs of these facilities have

been allocated between existing development and new development based on their percentage of build-out EBUs. As illustrated below in **Table 47**, 82.09% of the costs will be allocated to existing development and 17.91% of the costs will be allocated to new development. Based on this allocation between new and existing development, $1,392,170 of the $7,775,000 in Transportation facilities costs would be funded by the Municipal Developer Fee imposed on new development. The remaining $6,382,830 must be funded through other sources to be determined by the City.

Table 47: Transportation Facilities Cost Allocation Summary (Low) [1]

Development Type	Peak Hour Trips (EBUs)	Percentage Allocated	Facility Cost Allocation
Existing Development	7,980	82.09%	$6,382,830
New Development	1,741	17.91%	$1,392,170
Total	**9,721**	**100.00%**	**$7,775,000**

Note:

1. May not sum due to rounding.

To calculate the Municipal Developer Fees, DTA first determined the number of PHTs expected through 2040 based on the expected residential and non-residential growth in in the City. The analysis estimates that a maximum of 1,741 additional PHTs would be generated by the land use growth, as detailed in **Table 48** below. In this section, Peak Hour Trips (EBUs) are used instead of EDUs, and as explained in Section VI they are calculated the same way that EDUs were calculated in each of the previous sections. These calculations are presented in detail in **Appendix A**.

Table 48: Number of Trip Calculations (Low)

Land Use Type	Projected Development (Units)	Projected Development (Square Feet)	PHT Generation Rate [1]	Total PHTs (EBUs) [2]
Single-Family	403		0.99	399
Multi-Family	235		0.44	103
Commercial		403,573	2.51	1,014
Office		98,227	1.50	147
Industrial		128,983	0.52	66
Institutional		12,989	0.78	10
			Total	**1,741**

Note:

1 Projected PHTs per unit for residential and per 1,000 Square Feet for non-residential.
2 The service factor for Transportation is based on trips ends, so EBUs are used to allocate costs to future growth and generate fees.

H.2 Calculation Methodology

Table 49 presented below summarizes the cost per PHT, which is generated by dividing the cost to new development of $1,392,170 the number of PHTs that will be generated by new development (1,741). When accounting for the 1,741 planned PHTs in the City, the cost per PHT totals $800 as shown in the table below. The cost per PHT ($800) was then applied to the various land uses and their respective PHT trip generation rates to determine the proposed Municipal Developer Fee fees.

Table 49: Cost per Trip Estimate (Low)

Proposed Facilities Costs	Total
Cost Allocated to New Development	$1,392,170
Total PHTs Added by New Development	1,741
Cost Per PHT	**$800**

H.3 Fee Calculation

Expected revenue from new development was also calculated, ensuring that collected fees match the calculated cost responsibility of new development. For example, the maximum allowable fee for a single-family residence is calculated as follows: PHT rate [0.99] x costs per PHT [$800] = proposed Impact Fee per unit $792. Multi-family Developer Fees are calculated by multiplying the PHT rate [0.44] by the cost per PHT [$800], resulting in a proposed Impact Fee per unit of $352.

The fees for each of the other land use categories are calculated in the same manner, as outlined below in **Table 50**. The single-family and multi-family residential fees are calculated per housing unit and the non-residential fees are calculated per 1,000 square feet.

Table 50: Transportation Facilities Fee Calculations per Land Use Category (Low)

Land Use Type	PHT Generation Rate	Costs Per PHT	Municipal Developer Fees
Single-Family	0.99	$800	$792
Multi-Family	0.44	$800	$352
Commercial	2.51	$800	$2,010
Office	1.50	$800	$1,200
Industrial	0.52	$800	$412
Non-Residential	0.78	$800	$624

The total fee amounts to finance new development's share of the costs of facilities in the Facilities Needs Lists are summarized in **Table 51** below. It must be noted that the projects listed that will be funded by the proposed Municipal Developer Fees are not intended to fully offset the projected Transportation effects of development, as

developers will also undertake separate measures, such as traffic demand management programs, and localized mitigation measures, to help offset the traffic effects of new development. The proposed Municipal Developer Fee will not fully cover the cost of the capital projects and additional funding must be identified to implement many of the projects and programs identified herein, with a substantial share of that funding generated by existing residents, businesses, and/or roads system users.

Table 51: Transportation Development Facilities Fee Summary (Low)

Land Use	Fee Per Unit (1,000 Sq. Ft.)
Single-Family	$792
Multi-Family	$352
Commercial	$2,010
Office	$1,200
Industrial	$412
Institutional	$624

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA further recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News – Record ("ENR").

I Transportation – Medium Capital Costs

I.1 Transportation Faculties

The City's goal is to improve the City's Transportation Facilities over a period of approximately 20-years. Improvements focus on new bridges and additions to existing bridges, traffic and safety enhancements, improvements in safety at intersections, crosswalks, lighting, pedestrian improvements, and additional infrastructure. This additional infrastructure support is necessary to provide safe and efficient vehicular access throughout the City. The proposed Municipal Developers Fee is to help meet the transportation demand of new development through 2040. The City identified the need for the transportation infrastructure and equipment, as shown below in **Table 52**.

The Municipal Developer Fee will provide a source of revenue to the City to allow for the acquisition, installation, and construction of needed Transportation facilities, which in turn will both preserve the quality of life in the City and protect the health, safety, and welfare of the existing and future residents and employees. Transportation Fees will be calculated using the Plan-based approach discussed in Section VI.

Table 52: Purpose of Transportation Municipal Developer Fee (Medium)

Identify the Purpose of the Fee	Transportation Facilities
Identify of the use of the fee.	Various roadway improvements including, but not limited to, crosswalks, lighting, bridges, and road pedestrian safety.
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development will generate additional residents and employees who will create additional vehicular and non-vehicular traffic within the City limits. Streets will have to be improved or extended to meet the increased demand and to efficiently direct increased traffic flow. Thus, there is a relationship between new development and the need for new transportation facilities. Municipal Developer Fees collected from new development will be used exclusively for Traffic Facilities on the Facilities Needs List.

Identification of the facilities to be financed is a critical component of any Municipal Developer fee program. In the broadest sense, the purpose of Developer Fees is to protect the public health, safety, and general welfare by providing for Transportation facilities. The City has provided DTA with the list of Future Facilities (the "Facilities Needs List") to be included in the Fee Study. For the purposes of the City's Municipal program, the Facilities Needs List is intended to be the official public document

identifying the facilities eligible to be financed, in whole or in part, through the levy of a Municipal Developer fee on new development within the City. The Facilities Needs List is organized by facility element (or type) and includes cost information, as outlined in **Table 53** below.

The facilities included on the Facilities Needs List are provided by the City and reflect either the City's goals of maintaining and improving a specific area, or they are part of a more formal policy document, such as a General Plan, Capital Improvement Plan, etc. Specific estimated facility costs are provided by the City and used as a basis for determining the allocation of revenues between new and existing development.

The table below outlines the proposed facilities and respective costs along with any offsetting revenues. A list of Transportation facilities is included below and in **Appendix B** at the end of this Study. The cost estimates for the Transportation category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021.

Table 53: Transportation Facilities Costs (Medium)

Transportation Facilities – Medium Capital Costs	Facility Costs
Transportation Feasibility Study	$75,000
Additions to Existing Bridge and New Bridge	$2,000,000
Traffic Safety Enhancements at US340 and Augustine	$1,000,000
Augustine Ave. Trail	$200,000
Westend Gateway, WV 51/Summit Point Rd./W Washington St.	$5,000,000
Charles Street Improvements	$500,000
Transportation Facilities Subtotal	**$8,775,000**
Offsetting Revenue	$0.00
Transportation Facilities Total	**$8,775,000**

Transportation Developer Fees were calculated for each of the six (6) land use categories based on the number of PM Peak Hour Trips (PHTs) generated by each land use. As indicated earlier in Section VI, Peak Hour Trips are total vehicular trips entering and leaving a development project during the period between 4:00 pm and 6:00 pm which is the timeframe that experiences the highest sum of traffic volumes entering or leaving the development. Total PHTs were calculated by applying these trips rates to the various dwelling unit counts and non-residential square feet identified in the demographics section of this Fee Study. As discussed in Section VI, the Institute of Transportation Engineers (ITE) uses PM peak hours to define daily trip generation per dwelling unit (for residential units) and daily trip generation per 1,000 building square feet of each category of non-residential development.

All proposed Transportation facilities were sized to meet the needs of both existing and future residents and employees. Therefore, the costs of these facilities have

been allocated between existing development and new development based on their percentage of build-out EBUs. As illustrated below in **Table 54**, 82.09% of the costs will be allocated to existing development and 17.91% of the costs will be allocated to new development. Based on this allocation between new and existing development, $1,571,2280 of the $7,775,000 in Transportation facilities costs would be funded by the Municipal Developer Fee imposed on new development. The remaining $7,203,772 must be funded through other sources to be determined by the City.

Table 54: Transportation Facilities Cost Allocation Summary (Medium) [1]

Development Type	Peak Hour Trips (EBUs)	Percentage Allocated	Facility Cost Allocation
Existing Development	7,980	82.09%	$7,203,772
New Development	1,741	17.91%	$1,571,228
Total	**9,721**	**100.00%**	**$8,775,000**

Note:

1. May not sum due to rounding.

To calculate the Developer Fees, DTA first determined the number of PHTs expected through 2040 based on the expected residential and non-residential growth in in the City. The analysis estimates that a maximum of 1,741 additional PHTs would be generated by the land use growth, as detailed in **Table 55** below. In this section, Peak Hour Trips (EBUs) are used instead of EDUs, and as explained in Section VI they are calculated the same way that EDUs were calculated in each of the previous sections. These calculations are presented in detail in Appendix A.

Table 55: Number of Trip Calculations (Medium)

Land Use Type	Projected Development (Units)	Projected Development (Square Feet)	PHT Generation Rate [1]	Total PHTs (EBUs) [2]
Single-Family	403		0.99	399
Multi-Family	235		0.44	103
Commercial		403,573	2.51	1,014
Office		98,227	1.50	147
Industrial		128,983	0.52	66
Institutional		12,989	0.78	10
			Total	**1,741**

Note:

1. Projected PHTs per unit for residential and per 1,000 Square Feet for non-residential.
2. The service factor for Transportation is based on trips ends, so EBUs are used to allocate costs to future growth and generate fees.

I.2 Calculation Methodology

Table 56 presented below summarizes the cost per PHT, which is generated by dividing the cost to new development of $1,571,228 by the number of PHTs that will be generated by new development (1,741). When accounting for the 1,741 planned PHTs in the City, the cost per PHT totals $903. as shown in the table below. The cost per PHT ($903) was then applied to the various land uses and their respective PHT trip generation rates to determine the proposed Municipal Developer Fee fees.

Table 56: Cost per Trip Estimate (Medium)

Proposed Facilities Costs	Total
Cost Allocated to New Development	$1,571,228
Total PHTs Added by New Development	1,741
Cost Per PHT	**$903**

I.3 Fee Calculation

Expected revenue from new development was also calculated, ensuring that collected fees match the calculated cost responsibility of new development. For example, the maximum allowable fee for a single-family residence is calculated as follows: PHT rate [0.99] x costs per PHT [$903] = proposed Impact Fee per unit $894. Multi-family Developer Fees are calculated by multiplying the PHT rate [0.44] by the cost per PHT [$903], resulting in a proposed Impact Fee per unit of $397.

The fees for each of the other land use categories are calculated in the same manner, as outlined below in **Table 57**. The single-family and multi-family residential fees are calculated per housing unit and the non-residential fees are calculated per 1,000 square feet.

Table 57: Transportation Facilities Fee Calculations per Land Use Category (Medium)

Land Use Type	PHT Generation Rate	Costs Per PHT	Municipal Developer Fees
Single-Family	0.99	$903	$894
Multi-Family	0.44	$903	$397
Commercial	2.51	$903	$2,268
Office	1.50	$903	$1,354
Industrial	0.52	$903	$465
Non-Residential	0.78	$903	$704

The total fee amounts to finance new development's share of the costs of facilities in the Facilities Needs Lists are summarized in **Table 58** below. It must be noted that the projects listed in the Facilities Needs List that will be funded by the proposed

Municipal Developer Fee are not intended to fully offset the projected Transportation effects of development, as developers will also undertake separate measures, such as traffic demand management programs, and localized mitigation measures, to help offset the traffic effects of new development. The proposed Municipal Developer Fee will not fully cover the cost of the capital projects and additional funding must be identified to implement many of the projects and programs identified herein, with a substantial share of that funding generated by existing residents, businesses, and/or roads system users.

Table 58: Transportation Development Facilities Fee Summary (Medium)

Land Use	Fee Per Unit (1,000 Sq. Ft.)
Single-Family	$894
Multi-Family	$397
Commercial	$2,268
Office	$1,354
Industrial	$465
Institutional	$704

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA further recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News – Record ("ENR").

J Transportation – High Capital Costs

J.1 Transportation Facilities

The City's goal is to improve the City's Transportation Facilities over a period of approximately 20-years. Improvements focus on new bridges and additions to existing bridges, traffic and safety enhancements, improvements in safety at intersections, crosswalks, lighting, pedestrian improvements, and additional infrastructure. This additional infrastructure support is necessary to provide safe and efficient vehicular access throughout the City. The proposed Municipal Developer Fee is to help meet the transportation demand of new development through 2040. The City identified the need for the transportation infrastructure and equipment, as shown below in **Table 59**.

The Municipal Developer Fee will provide a source of revenue to the City to allow for the acquisition, installation, and construction of needed Transportation facilities, which in turn will both preserve the quality of life in the City and protect the health, safety, and welfare of the existing and future residents and employees. Transportation Fees will be calculated using the Plan-based approach discussed in Section VI.

Table 59: Purpose of Transportation Municipal Developer Fee (High)

Identify the Purpose of the Fee	Transportation Facilities
Identify of the use of the fee.	Various roadway improvements including, but not limited to, crosswalks, lighting, bridges, and road pedestrian safety.
Demonstrate how there is a reasonable relationship between the need for the public facility, use of the fee, and type of development project on which the fee is imposed.	New residential and non-residential development will generate additional residents and employees who will create additional vehicular and non-vehicular traffic within the City limits. Streets will have to be improved or extended to meet the increased demand and to efficiently direct increased traffic flow. Thus, there is a relationship between new development and the need for new transportation facilities. Municipal Developer Fees collected from new development will be used exclusively for Traffic Facilities on the Facilities Needs List.

Identification of the facilities to be financed is a critical component of any Municipal Developer fee program. In the broadest sense, the purpose of Developer Fees is to protect the public health, safety, and general welfare by providing for Transportation facilities. The City has provided DTA with the list of Future Facilities (the "Facilities Needs List") to be included in the Fee Study. For the purposes of the City's Municipal program, the Facilities Needs List is intended to be the official public document

identifying the facilities eligible to be financed, in whole or in part, through the levy of a Municipal Developer fee on new development within the City. The Facilities Needs List is organized by facility element (or type) and includes cost information, as outlined in **Table 60** below.

The facilities included on the Facilities Needs List are provided by the City and reflect either the City's goals of maintaining and improving a specific area, or they are part of a more formal policy document, such as a General Plan, Capital Improvement Plan, etc. Specific estimated facility costs are provided by the City and used as a basis for determining the allocation of revenues between new and existing development.

The table below outlines the proposed facilities and respective costs along with any offsetting revenues. A list of Transportation facilities is included below and in **Appendix B** at the end of this Study. The cost estimates for the Transportation category were provided by the City and based on the City's Growth-Related Capital Improvements Projects – Developer Fee Analysis as of November 30, 2021.

Table 60: Transportation Facilities Costs (High)

Transportation Facilities – High Capital Costs	Facility Costs
Transportation Feasibility Study	$75,000
Additions to Existing Bridge and New Bridge	$2,000,000
Traffic Safety Enhancements at US340 and Augustine	$1,000,000
Augustine Ave. Trail	$200,000
Westend Gateway, WV 51/Summit Point Rd./W Washington St.	$6,000,000
Charles Street Improvements	$500,000
Transportation Facilities Subtotal	**$9,775,000**
Offsetting Revenue	$0.00
Transportation Facilities Total	**$9,775,000**

Transportation Developer Fees were calculated for each of the six (6) land use categories based on the number of PM Peak Hour Trips (PHTs) generated by each land use. As indicated earlier in Section VI, Peak Hour Trips are total vehicular trips entering and leaving a development project during the period between 4:00 pm and 6:00 pm which is the timeframe that experiences the highest sum of traffic volumes entering or leaving the development. Total PHTs were calculated by applying these trips rates to the various dwelling unit counts and non-residential square feet identified in the demographics section of this Fee Study. As discussed in Section VI, the Institute of Transportation Engineers (ITE) uses PM peak hours to define daily trip generation per dwelling unit (for residential units) and daily trip generation per 1,000 building square feet of each category of non-residential development.

All proposed Transportation facilities were sized to meet the needs of both existing and future residents and employees. Therefore, the costs of these facilities have

been allocated between existing development and new development based on their percentage of build-out EBUs. As illustrated below in **Table 61**, 82.09% of the costs will be allocated to existing development and 17.91% of the costs will be allocated to new development. Based on this allocation between new and existing development, $1,750,285 of the $9,775,000 in Transportation facilities costs would be funded by the Municipal Developer Fee imposed on new development. The remaining $8,024,285 must be funded through other sources to be determined by the City.

Table 61: Transportation Facilities Cost Allocation Summary (High) [1]

Development Type	Peak Hour Trips (EBUs)	Percentage Allocated	Facility Cost Allocation
Existing Development	7,980	82.09%	$8,024,715
New Development	1,741	17.91%	$1,750,285
Total	**9,721**	**100.00%**	**$9,775,000**

Note:

1. May not sum due to rounding.

To calculate the Developer Fees, DTA first determined the number of PHTs expected through 2040 based on the expected residential and non-residential growth in in the City. The analysis estimates that a maximum of 1,741 additional PHTs would be generated by the land use growth, as detailed in **Table 62** below. In this section, Peak Hour Trips (EBUs) are used instead of EDUs, and as explained in Section VI they are calculated the same way that EDUs were calculated in each of the previous sections. These calculations are presented in detail in **Appendix A**.

Table 62: Number of Trip Calculations (High)

Land Use Type	Projected Development (Units)	Projected Development (Square Feet)	PHT Generation Rate [1]	Total PHTs (EBUs)[2]
Single-Family	403		0.99	399
Multi-Family	235		0.44	103
Commercial		403,573	2.51	1,014
Office		98,227	1.50	147
Industrial		128,983	0.52	66
Institutional		12,989	0.78	10
			Total	**1,741**

Note:

1. Projected PHTs per unit for residential development and per 1,000 Square Feet for non-residential development.
2. The service for Transportation facilities is based on trips ends, so EBUs are used to allocated costs and generate fees.

J.2 Calculation Methodology

Table 63 presented below summarizes the cost per PHT, which is generated by dividing the cost to new development of $1,750,285 by the number of PHTs that will be generated by new development (1,741). When accounting for the 1,741 planned PHTs in the City, the cost per PHT totals $1,006 as shown in the table below. The cost per PHT ($1,006) was then applied to the various land uses and their respective PHT trip generation rates to determine the proposed Municipal Developer Fee fees.

Table 63: Cost per Trip Estimate (High)

Proposed Facilities Costs	Total
Cost Allocated to New Development	$1,750,285
Total PHTs Added by New Development	1,741
Cost Per PHT	**$1,006**

J.3 Fee Calculation

Expected revenue from new development was also calculated, ensuring that collected fees match the calculated cost responsibility of new development. For example, the maximum allowable fee for a single-family residence is calculated as follows: PHT rate [0.99] x costs per PHT [$1,006] = proposed Impact Fee per unit $995. Multi-family Developer Fees are calculated by multiplying the PHT rate [0.44] by the cost per PHT [$1,006], resulting in a proposed Impact Fee per unit of $442.

The fees for each of the other land use categories are calculated in the same manner, as outlined below in **Table 64**. The single-family and multi-family residential fees are calculated per housing unit and the non-residential fees are calculated per 1,000 square feet.

Table 64: Transportation Facilities Fee Calculations per Land Use Category (High)

Land Use Type	PHT Generation Rate	Costs Per PHT	Municipal Developer Fees
Single-Family	0.99	$1,006	$995
Multi-Family	0.44	$1,006	$442
Commercial	2.51	$1,006	$2,526
Office	1.50	$1,006	$1,508
Industrial	0.52	$1,006	$518
Non-Residential	0.78	$1,006	$784

The total fee amounts to finance new development's share of the costs of facilities in the Facilities Needs Lists are summarized in **Table 65** below. It must be noted that the projects listed in the Facilities Needs List that will be funded by the proposed

Municipal Developer Fee are not intended to fully offset the projected Transportation effects of development, as developers will also undertake separate measures, such as traffic demand management programs, and localized mitigation measures, to help offset the traffic effects of new development. The proposed Municipal Developer Fee will not fully cover the cost of the capital projects and additional funding must be identified to implement many of the projects and programs identified herein, with a substantial share of that funding generated by existing residents, businesses, and/or roads system users.

Table 65: Transportation Development Facilities Fee Summary (High)

Land Use	Fee Per Unit (1,000 Sq. Ft.)
Single-Family	$995
Multi-Family	$442
Commercial	$2,526
Office	$1,508
Industrial	$518
Institutional	$784

The cost estimates for future facilities used in this fee study are presented in 2022 dollars. DTA further recommends that, after adoption, the fee should be reviewed each year and adjusted by the Construction Cost Index ("CCI"). The recommended construction cost index is based upon the Building Cost Index ("BCI") average produced by the Engineering News – Record ("ENR").

VIII SUMMARY OF FEES

The total proposed fee amounts to finance new development's share of the costs of new facilities are summarized below. These calculations are based on best practices and with the specific purpose of establishing a nexus between anticipated development and Future Facilities for the City through 2040.

Table 66: Proposed Municipal Developer Fee Summary
Lowest Cost Capital Improvement Scenario [2]

Land Use [1]	Fire and Rescue	Police	Municipal Facilities	Library Facilities	Parks and Recreation	Transportation	Total
Single-Family	$126	$201	$1,107	$62	$499	$792	$2,787
Multi-Family	$125	$200	$1,098	$62	$495	$352	$2,331
Commercial	$28	$45	$247	$0	$0	$2,010	$2,329
Office	$30	$47	$260	$0	$0	$1,200	$1,536
Industrial	$17	$26	$145	$0	$0	$412	$600
Institutional	$19	$31	$169	$0	$0	$624	$842

Notes:

1. Residential fees are per unit and non-residential fees are per 1,000 square feet.
2. Total Capital Improvements $15,275,000.

Table 67: Proposed Municipal Developer Fee Summary
Medium Cost Capital Improvement Scenario [2]

Land Use [1]	Fire and Rescue	Police	Municipal Facilities	Library Facilities	Parks and Recreation	Transportation	Total
Single-Family	$126	$201	$1,359	$62	$499	$894	$3,140
Multi-Family	$125	$200	$1,348	$62	$495	$397	$2,626
Commercial	$28	$45	$303	$0	$0	$2,268	$2,644
Office	$30	$47	$319	$0	$0	$1,354	$1,749
Industrial	$17	$26	$178	$0	$0	$465	$686
Institutional	$19	$31	$207	$0	$0	$704	$961

Notes:

1. Residential fees are per unit and non-residential fees are per 1,000 square feet.
2. Total Capital Improvements $17,275,000.

Table 68: Proposed Municipal Developer Fee Summary
Highest Cost Capital Improvement Scenario[2]

Land Use [2]	Fire and Rescue	Police	Municipal Facilities	Library Facilities	Parks and Recreation	Transportation	Total
Single-Family	$126	$201	$1,610	$62	$499	$995	$3,494
Multi-Family	$125	$200	$1,597	$62	$495	$442	$2,921
Commercial	$28	$45	$359	$0	$0	$2,526	$2,958
Office	$30	$47	$378	$0	$0	$1,508	$1,963
Industrial	$17	$26	$211	$0	$0	$518	$772
Institutional	$19	$31	$245	$0	$0	$784	$1,079

Notes:

1. Residential fees are per unit and non-residential fees are per 1,000 square feet.
2. Total Capital Improvements $19,275,000.

APPENDIX A

City of Charles Town, WV
Municipal Developer Fee Justification Study

FEE DERIVATION WORKSHEETS

APPENDIX A-1
Charles Town, West Virginia
FIRE AND RESCUE FEE CALCULATION

I. Existing EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	4,117	2.52	1.00	1,631	1,631
Multi Family Residential	2,377	2.50	0.99	949	941
Commercial	1,091	0.56	0.22	1,939,237	432
Office	280	0.59	0.23	472,000	111
Industrial	206	0.33	0.13	619,787	81
Institutional	24	0.38	0.15	62,415	10
Total	**8,094**				**3,206**

II. Projected EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	1,019	2.52	1.00	403	403
Multi Family Residential	588	2.50	0.99	235	233
Office	227	0.56	0.22	403,573	90
Commercial	58	0.59	0.23	98,227	23
Industrial	43	0.33	0.13	128,983	17
Institutional	5	0.38	0.15	12,989	2
Total	**1,940**				**768**

III. Projected Fire Facilities Costs

Facility		Facility Cost
Fire and Rescue Facilities	$	500,000
Offsetting Revenues		
Total Facilities Cost	**$**	**500,000**

IV. Allocation of New Development to New and Existing Facilities

Development	EDU's	Percentage of Cost Allocated		Percentage of Cost Allocated
Existing Development	3,206	80.67%	$	403,348
New Development	768	19.33%	$	96,652
	3,975	**100.00%**	**$**	**500,000**

V. Allocation of New Development

Facility	Number of Projected EDUs	Cost to New Development		Cost per EDU
Fire Facilities	768	$	96,652	$ 126

VI. Developer Fee per Unit

Land Use Type	EDU's per Unit	Fee Per Unit/ Per 1,000 SF	Total Units/ Non-Res SF	Costs Financed by DIF
Single Family Residential	1.00	$126	403	$50,759
Multi Family Residential	0.99	$125	235	$29,300
Commercial	0.22	$28	403,573	$11,314
Office	0.23	$30	98,227	$2,899
Industrial	0.13	$17	128,983	$2,131
Institutional	0.15	$19	12,989	$249
Total				**$96,652**

VII. Developer Fee Summary

Land Use Category	Fee Per Unit/ Per 1,000 SF
Single Family Residential	$126
Multi Family Residential	$125
Commercial	$28
Office	$30
Industrial	$17
Institutional	$19

APPENDIX A-2
Charles Town, West Virginia
POLICE FEE CALCULATION

I. Existing EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	4,117	2.52	1.00	1,631	1,631
Multi Family Residential	2,377	2.50	0.99	949	941
Commercial	1,091	0.56	0.22	1,939,237	432
Office	280	0.59	0.23	472,000	111
Industrial	206	0.33	0.13	619,787	81
Institutional	24	0.38	0.15	62,415	10
Total	**8,094**				**3,206.2843**

II. Projected EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	1,019	2.52	1.00	403	403
Multi Family Residential	588	2.50	0.99	235	233
Office	227	0.56	0.22	403,573	90
Commercial	58	0.59	0.23	98,227	23
Industrial	43	0.33	0.13	128,983	17
Institutional	5	0.38	0.15	12,989	2
Total	**1,940**				**768.30408**

III. Projected Fire Facilities Costs

Facility		Facility Cost
Police Facilities	$	800,000
Offsetting Revenues		
Total Facilities Cost	**$**	**800,000**

IV. Allocation of New Development to New and Existing Facilities

Development	EDU's	Percentage of Cost Allocated		Percentage of Cost Allocated
Existing Development	3,206	80.67%	$	645,357
New Development	768	19.33%	$	154,643
	3,975	**100.00%**	**$**	**800,000**

V. Allocation of New Development

Facility	Number of Projected EDUs	Cost to New Development		Cost per EDU
Police Facilities	768	$	154,643	$ 201

VI. Developer Fee per Unit

Land Use Type	EDU's per Unit	Fee Per Unit/ Per 1,000 SF	Total Units/ Non-Res SF	Costs Financed by DIF
Single Family Residential	1.00	$201	403	$81,214
Multi Family Residential	0.99	$200	235	$46,880
Commercial	0.22	$45	403,573	$18,103
Office	0.23	$47	98,227	$4,638
Industrial	0.13	$26	128,983	$3,410
Institutional	0.15	$31	12,989	$398
Total				**$154,643**

VII. Developer Fee Summary

Land Use Category	Fee Per Unit/ Per 1,000 SF
Single Family Residential	$201
Multi Family Residential	$200
Commercial	$45
Office	$47
Industrial	$26
Institutional	$31

APPENDIX A-3
Charles Town, West Virginia
MUNICIPAL FACILITIES FEE CALCULATION
(Low Capital Improvement Cost Scenario)

I. Existing EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	4,117	2.52	1.00	1,631	1,631
Multi Family Residential	2,377	2.50	0.99	949	941
Commercial	1,091	0.56	0.22	1,939,237	432
Office	280	0.59	0.23	472,000	111
Industrial	206	0.33	0.13	619,787	81
Institutional	24	0.38	0.15	62,415	10
Total	**8,094**				**3,206**

II. Projected EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	1,019	2.52	1.00	403	403
Multi Family Residential	588	2.50	0.99	235	233
Office	227	0.56	0.22	403,573	90
Commercial	58	0.59	0.23	98,227	23
Industrial	43	0.33	0.13	128,983	17
Institutional	5	0.38	0.15	12,989	2
Total	**1,940**				**768**

III. Projected Municipal Facilities Costs

Facility		Facility Cost
Municipal Facilities	$	4,400,000
Offsetting Revenues		
Total Facilities Cost	**$**	**4,400,000**

IV. Allocation of New Development to New and Existing Facilities

Development	EDU's	Percentage of Cost Allocated		Percentage of Cost Allocated
Existing Development	3,206	80.67%	$	3,549,462
New Development	768	19.33%	$	850,538
	3,975	**100.00%**	**$**	**4,400,000**

V. Allocation of New Development

Facility	Number of Projected	Cost to New Development		Cost per EDU
Municipal Facilities	768	$	850,538	$ 1,107

VI. Developer Fee per Unit

Land Use Type	EDU's per Unit	Fee Per Unit/ Per 1,000 SF	Total Units/ Non-Res SF	Costs Financed by DIF
Single Family Residential	1.00	$1,107	403	$446,679
Multi Family Residential	0.99	$1,098	235	$257,842
Commercial	0.22	$247	403,573	$99,566
Office	0.23	$260	98,227	$25,507
Industrial	0.13	$145	128,983	$18,754
Institutional	0.15	$169	12,989	$2,190
Total				**$850,538**

APPENDIX A-3
Charles Town, West Virginia
MUNICIPAL FEE CALCULATION
(Medium Capital Improvement Cost Scenario)

I. Existing EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	4,117	2.52	1.00	1,631	1,631
Multi Family Residential	2,377	2.50	0.99	949	941
Commercial	1,091	0.56	0.22	1,939,237	432
Office	280	0.59	0.23	472,000	111
Industrial	206	0.33	0.13	619,787	81
Institutional	24	0.38	0.15	62,415	10
Total	**8,094**				**3,206**

II. Projected EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	1,019	2.52	1.00	403	403
Multi Family Residential	588	2.50	0.99	235	233
Office	227	0.56	0.22	403,573	90
Commercial	58	0.59	0.23	98,227	23
Industrial	43	0.33	0.13	128,983	17
Institutional	5	0.38	0.15	12,989	2
Total	**1,940**				**768**

III. Projected Municipal Facilities Costs

Facility		Facility Cost
Municipal Facilities	$	5,400,000
Offsetting Revenues		
Total Facilities Cost	**$**	**5,400,000**

IV. Allocation of New Development to New and Existing Facilities

Development	EDU's	Percentage of Cost Allocated		Percentage of Cost Allocated
Existing Development	3,206	80.67%	$	4,356,158
New Development	768	19.33%	$	1,043,842
	3,975	**100.00%**	**$**	**5,400,000**

V. Allocation of New Development

Facility	Number of Projected EDU	Cost to New Development	Cost per EDU
Municipal Facilities	768	$ 1,043,842	$ 1,359

VI. Developer Fee per Unit

Land Use Type	EDU's per Unit	Fee Per Unit/ Per 1,000 SF	Total Units/ Non-Res SF	Costs Financed by DIF
Single Family Residential	1.00	$1,359	403	$548,196
Multi Family Residential	0.99	$1,348	235	$316,442
Commercial	0.22	$303	403,573	$122,194
Office	0.23	$319	98,227	$31,305
Industrial	0.13	$178	128,983	$23,016
Institutional	0.15	$207	12,989	$2,688
Total				**$1,043,842**

VII. Developer Impact Fee Summary

Land Use Category	Fee Per Unit/ Per 1,000 SF
Single Family Residential	$1,359
Multi Family Residential	$1,348
Commercial	$303
Office	$319
Industrial	$178
Institutional	$207

APPENDIX A-3
Charles Town, West Virginia
MUNICIPAL FEE CALCULATION
(High Capital Improvement Cost Scenario)

I. Existing EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	4,117	2.52	1.00	1,631	1,631
Multi Family Residential	2,377	2.50	0.99	949	941
Commercial	1,091	0.56	0.22	1,939,237	432
Office	280	0.59	0.23	472,000	111
Industrial	206	0.33	0.13	619,787	81
Institutional	24	0.38	0.15	62,415	10
Total	**8,094**				**3,206**

II. Projected EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit/ Persons Served per 1,000 Non-Res. SF	EDUs per Unit/ per 1,000 Non-Res. SF	Number of Units/ Non-Res. SF	Total Number of EDUs
Single Family Residential	1,019	2.52	1.00	403	403
Multi Family Residential	588	2.50	0.99	235	233
Office	227	0.56	0.22	403,573	90
Commercial	58	0.59	0.23	98,227	23
Industrial	43	0.33	0.13	128,983	17
Institutional	5	0.38	0.15	12,989	2
Total	**1,940**				**768**

III. Projected Municipal Facilities Costs

Facility		Facility Cost
Municipal Facilities	$	6,400,000
Offsetting Revenues		
Total Facilities Cost	**$**	**6,400,000**

IV. Allocation of New Development to New and Existing Facilities

Development	EDU's	Percentage of Cost Allocated		Percentage of Cost Allocated
Existing Development	3,206	80.67%	$	5,162,854
New Development	768	19.33%	$	1,237,146
	3,975	**100.00%**	**$**	**6,400,000**

V. Allocation of New Development

Facility	Number of Projected EDU		Cost to New Development		Cost per EDU
Municipal Facilities	768	$	1,237,146	$	1,610

VI. Developer Fee per Unit

Land Use Type	EDU's per Unit	Fee Per Unit/ Per 1,000 SF	Total Units/ Non-Res SF	Costs Financed by DIF
Single Family Residential	1.00	$1,610	403	$649,714
Multi Family Residential	0.99	$1,597	235	$375,042
Commercial	0.22	$359	403,573	$144,823
Office	0.23	$378	98,227	$37,102
Industrial	0.13	$211	128,983	$27,279
Institutional	0.15	$245	12,989	$3,186
Total				**$1,237,146**

VII. Developer Impact Fee Summary

Land Use Category	Fee Per Unit/ Per 1,000 SF
Single Family Residential	$1,610
Multi Family Residential	$1,597
Commercial	$359
Office	$378
Industrial	$211
Institutional	$245

APPENDIX A-4
Charles Town, West Virginia
LIBRARY FACILITIES FEE CALCULATION

I. Existing EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit	EDUs per Unit	Number of Units	Total Number of EDUs
Single Family Residential	4,117	2.52	1.00	1,631	1,631
Multi Family Residential	2,377	2.50	0.99	949	941
Total	**6,494**				**2,572.482**

II. Projected EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit	EDUs per Unit	Number of Units	Total Number of EDUs
Single Family Residential	1,019	2.52	1.00	403	403
Multi Family Residential	588	2.50	0.99	235	233
Total	**1,607**				**636.4040**

III. Projected Fire Facilities Costs

Facility		Facility Cost
Library Facilities	$	200,000
Offsetting Revenues		
Total Facilities Cost	**$**	**200,000**

IV. Allocation of New Development to New and Existing Facilities

Development	EDU's	Percentage of Cost Allocated		Percentage of Cost Allocated
Existing Development	2,572	80.17%	$	160,335
New Development	636	19.83%	$	39,665
	3,209	**100.00%**	**$**	**200,000**

V. Allocation of New Development

Facility	Number of Projected EDU		Cost to New Development		Cost per EDU
Library Facilities	636	$	39,665	$	62

VI. Developer Fee per Unit

Land Use Type	EDU's per Unit	Fee Per Unit/ Per 1,000 SF	Total Units/ Non-Res SF	Costs Financed by DIF
Single Family Residential	1.00	$62.33	403	$25,148
Multi Family Residential	0.99	$61.83	235	$14,517
Total				**$39,665**

VII. Developer Fee Summary

Land Use Category	Fee Per Unit
Single Family Residential	$62.33
Multi Family Residential	$61.83

APPENDIX A-5
Charles Town, West Virginia
PARKS AND RECREATION FEE CALCULATION

Existing EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit	EDUs per Unit/	Number of Units	Total Number of EDUs
Single Family Residential	4,117	2.52	1.00	1,631	1,631
Multi Family Residential	2,377	2.50	0.99	949	941
Total	**6,494**				**2,572**

Projected EDU Calculation

Land Use Type	Number of Persons Served	Residents per Unit	EDUs per Unit/	Number of Units	Total Number of EDUs
Single Family Residential	1,019	2.52	1.00	403	403
Multi Family Residential	588	2.50	0.99	235	233
Total	**1,607**				**636.404036**

III. Projected Fire Facilities Costs

Facility		Facility Cost
Parks and Recreation Facilities	$	1,600,000
Offsetting Revenues		
Total Facilities Cost	**$**	**1,600,000**

IV. Allocation of New Development to New and Existing Facilities

Development	EDU's	Percentage of Cost Allocated		Percentage of Cost Allocated
Existing Development	2,572	80.17%	$	1,282,679
New Development	636	19.83%	$	317,321
	3,209	**100.00%**	**$**	**1,600,000**

V. Allocation of New Development

Facility	Number of Projected EDUs		Cost to New Development		Cost per EDU
Parks Facilities	636	$	317,321	$	499

VI. Developer Fee per Unit

Land Use Type	EDU's per Unit	Fee Per Unit/ Per 1,000 SF	Total Units/ Non-Res SF	Costs Financed by DIF
Single Family Residential	1.00	$499	403	$201,187
Multi Family Residential	0.99	$495	235	$116,134
Total				**$317,321**

VII. Developer Fee Summary

Land Use Category	Fee Per Unit
Single Family Residential	$499
Multi Family Residential	$495

APPENDIX A-6
Charles Town, West Virginia
TRANSPORTATION FEE CALCULATION
(Low Capital Improvement Cost Scenario)

I. Existing EDU Calculation

Land Use Type	Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Number of Existing Units	Existing Non-Residential S.F.	Peak Hour Trips EBUs (Per Unit/1,000 SF)
Single-Family	0.99	1,631		1,615
Multi-Family	0.44	949		418
Commercial	2.51		1,939,237	4,872
Office	1.50		472,000	708
Industrial	0.52		619,787	319
Institutional	0.78		62,415	49
Total				**7,980**

II. Future EDU Calculation

Land Use Type	Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Number of Projected Units	Projected Non-Residential S.F.	Peak Hour Trips EBUs (Per Unit/1,000 SF)
Single-Family	0.99	403		399
Multi-Family	0.44	235		103
Commercial	2.51		403,573	1,014
Office	1.50		98,227	147
Industrial	0.52		128,983	66
Institutional	0.78		12,989	10
Total				**1,741**

III. Proposed Facilities Cost

Facility	Facility Cost
Transportation Facilities Cost	**$7,775,000**
Offsetting Revenues	**$0**
Total Facilities Cost	**$7,775,000**

IV. Allocation of Facilities to Existing and New Development (based on Daily Trips)

Development	Peak Hour Trips (EBUs)	Percentage of Cost Allocated	Facility Cost
Existing Development	7,980	82.09%	$6,382,830
New Development	1,741	17.91%	$1,392,170
Total Facilities Cost	9,721	100.00%	**$7,775,000**

V. Allocation of Facilities to New Development (based on New EDUs)

Facility	Projected Daily Trips	Facility Cost Allocated to New Development	Facilities Cost Per Daily Trip
Transportation Facilities Cost	1,741	$1,392,170	$800
Total Facilities Cost per Daily Trip	**1,741**		**$800**

VI. Developer Fees and Cost Financed by Fees per Unit/per 1,000 Non-Res. S.F.

Land Use Type	Estimated Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Fee per Unit	Fees per 1,000 Non-Res. S.F.	Cost Financed by Impact Fees
Single-Family	0.99	$792		$319,489
Multi-Family	0.44	$352		$82,620
Commercial	2.51		$2,010	$810,986
Office	1.50		$1,200	$117,845
Industrial	0.52		$412	$53,128
Institutional	0.78		$624	$8,103
Initial Allocation to New Development				**$1,392,170**
Total Allocated to Existing Development				$6,382,830
Total Facilities Costs				**$7,775,000**

VII. Developer Fee Summary

Land Use Category	Fees
Single-Family	$792
Multi-Family	$352
Commercial	$2,010
Office	$1,200
Industrial	$412
Institutional	$624

APPENDIX A-6
Charles Town, West Virginia
TRANSPORTATION FEE CALCULATION
(Medium Capital Improvement Cost Scenario)

I. Existing EDU Calculation

Land Use Type	Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Number of Existing Units	Existing Non-Residential S.F.	Peak Hour Trips EBUs (Per Unit/1,000 SF)
Single-Family	0.99	1,631		1,615
Multi-Family	0.44	949		418
Commercial	2.51		1,939,237	4,872
Office	1.50		472,000	708
Industrial	0.52		619,787	319
Institutional	0.78		62,415	49
Total				**7,980**

II. Future EDU Calculation

Land Use Type	Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Number of Projected Units	Projected Non-Residential S.F.	Peak Hour Trips EBUs (Per Unit/1,000 SF)
Single-Family	0.99	403		399
Multi-Family	0.44	235		103
Commercial	2.51		403,573	1,014
Office	1.50		98,227	147
Industrial	0.52		128,983	66
Institutional	0.78		12,989	10
Total				**1,741**

III. Proposed Facilities Cost

Facility	Facility Cost
Transportation Facilities Cost	**$8,775,000**
Offsetting Revenues	**$0**
Total Facilities Cost	**$8,775,000**

9,721

IV. Allocation of Facilities to Existing and New Development (based on Daily Trips)

Development	Peak Hour Trips (EBUs)	Percentage of Cost Allocated	Facility Cost
Existing Development	7,980	82.09%	$7,203,772
New Development	1,741	17.91%	$1,571,228
Total Facilities Cost	9,721	100.00%	**$8,775,000**

V. Allocation of Facilities to New Development (based on New EDUs)

Facility	Projected Daily Trips ew Development	Facility Cost Allocated to	Facilities Cost Per Daily Trip
Transportation Facilities Cost	1,741	$1,571,228	$903
Total Facilities Cost per Daily Trip	**1,741**		**$903**

VI. Developer Fees and Cost Financed by Fees per Unit/per 1,000 Non-Res. S.F.

Land Use Type	Estimated Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Fee per Unit	Fees per 1,000 Non-Res. S.F.	Cost Financed by Impact Fees
Single-Family	0.99	$894		$360,580
Multi-Family	0.44	$397		$93,246
Commercial	2.51		$2,268	$915,293
Office	1.50		$1,354	$133,001
Industrial	0.52		$465	$59,962
Institutional	0.78		$704	$9,145
Initial Allocation to New Development				**$1,571,228**
Total Allocated to Existing Development				$7,203,772
Total Facilities Costs				**$8,775,000**

VII. Developer Fee Summary

Land Use Category	Fees
Single-Family	$894
Multi-Family	$397
Commercial	$2,268
Office	$1,354
Industrial	$465
Institutional	$704

APPENDIX A-6
Charles Town, West Virginia
TRANSPORTATION FEE CALCULATION
(High Capital Improvement Cost Scenario)

I. Existing EDU Calculation

Land Use Type	Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Number of Existing Units	Existing Non-Residential S.F.	Peak Hour Trips EBUs (Per Unit/1,000 SF)
Single-Family	0.99	1,631		1,615
Multi-Family	0.44	949		418
Commercial	2.51		1,939,237	4,872
Office	1.50		472,000	708
Industrial	0.52		619,787	319
Institutional	0.78		62,415	49
Total				**7,980**

II. Future EDU Calculation

Land Use Type	Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Number of Projected Units	Projected Non-Residential S.F.	Peak Hour Trips EBUs (Per Unit/1,000 SF)
Single-Family	0.99	403		399
Multi-Family	0.44	235		103
Commercial	2.51		403,573	1,014
Office	1.50		98,227	147
Industrial	0.52		128,983	66
Institutional	0.78		12,989	10
Total				**1,741**

III. Proposed Facilities Cost

Facility	Facility Cost
Transportation Facilities Cost	**$9,775,000**
Offsetting Revenues	**$0**
Total Facilities Cost	**$9,775,000**

IV. Allocation of Facilities to Existing and New Development (based on Daily Trips)

Development	Peak Hour Trips (EBUs)	Percentage of Cost Allocated	Facility Cost
Existing Development	7,980	82.09%	$8,024,715
New Development	1,741	17.91%	$1,750,285
Total Facilities Cost	9,721	100.00%	**$9,775,000**

V. Allocation of Facilities to New Development (based on New EDUs)

Facility	Projected Daily Trips ew Development	Facility Cost Allocated to	Facilities Cost Per Daily Trip
Transportation Facilities Cost	1,741	$1,750,285	$1,006
Total Facilities Cost per Daily Trip	**1,741**		**$1,006**

VI. Developer Fees and Cost Financed by Fees per Unit/per 1,000 Non-Res. S.F.

Land Use Type	Estimated Trip Generation Rate per Unit/ per 1,000 Non-Res. S.F.	Fee per Unit	Fees per 1,000 Non-Res. S.F.	Cost Financed by Impact Fees
Single-Family	0.99	$995		$401,672
Multi-Family	0.44	$442		$103,873
Commercial	2.51		$2,526	$1,019,599
Office	1.50		$1,508	$148,158
Industrial	0.52		$518	$66,795
Institutional	0.78		$784	$10,188
Initial Allocation to New Development				**$1,750,285**
Total Allocated to Existing Development				$8,024,715
Total Facilities Costs				**$9,775,000**

VII. Developer Fee Summary

Land Use Category	Fees
Single-Family	$995
Multi-Family	$442
Commercial	$2,526
Office	$1,508
Industrial	$518
Institutional	$784

APPENDIX B

City of Charles Town, WV
Municipal Developer Fee Justification Study

FACILITIES NEEDS LIST

Appendix B-1
DEVELOPER FEES
CITY OF CHARLES TOWN WV
PUBLIC FACILITIES NEEDS LIST THROUGH 2040
(Low Capital Cost Improvement Scenario)

Facility Name	Total Cost for Facility	Off-setting Revenues	Net Cost to City	Percent of Cost Allocated to New Development	Cost Allocated to New Development	Policy Background or Objective
Fire						
Equipment and Facility upgrade due to growth for both fire companies - Independent and Citizens Fire Companies	**$500,000**		$ 500,000	19.33%	$96,652	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Fire Facilities Subtotal	**$ 500,000**	**$ -**	**$ 500,000**			
Police						
Vehicles and Equipment	$800,000	$ -	$ 800,000	19.33%	$154,643	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Police Facilities Subtotal	**$ 800,000**	**$ -**	**$ 800,000**			
Municipal Facilities						
Expansion of Police Headquarters - added security features and build out of existing CTUB space to accommodate larger police force	$300,000	$ -	$ 300,000	19.33%	$57,991	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
City Hall Expansion / Renovations - Growing community will require additional space to accommodate staff. 101 W Washington St.	$3,000,000	$ -	$ 3,000,000	19.33%	$579,912	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Maintenance yard and facility - new facility will be needed to house and maintain additional equipment required to serve a larger community - Water Street	$750,000	$ -	$ 750,000	19.33%	$144,978	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Storm Water equipment - Replacement street sweeper to service additional roads / gutters resulting from growth; sweeper will preserve stormwater system by preventing debris from entering - Water Street	$350,000	$ -	$ 350,000	19.33%	$67,656	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Municipal Facilities Subtotal	**$ 4,400,000**	**$ -**	**$ 4,400,000**			
Library Facilities						
Placeholder project - Equipment to accommodate future growth such as the acquisition of books and materials, computer equipment, required replacement of facilities and capital improvements,	$200,000	$ -	$ 200,000	19.83%	$39,665	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Library Facilities Subtotal	**$ 200,000**	**$ -**	**$200,000**			

Parks and Recreation							
Expansion of Pool to accommodate growth - Jefferson Memorial Park	$700,000	$ -	$ 700,000	19.83%	$138,828	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Acquisition of parkland and amenities to accommodate future growth - includes tennis courts, pickle ball courts, play fields, play equipment	$500,000	$ -	$ 500,000	19.83%	$99,163	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Walking Bridges that connect existing parks on the west end of town. Evitts Run Park and Happy Retreat	$400,000	$ -	$ 400,000	19.83%	$79,330	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Offsetting Revenues							
Parks Facilities Subtotal	**$ 1,600,000**	**$ -**	**$1,600,000**				
Transportation							
Feasibility Study to examine options for connecting Wards 2 and 4 to downtown	$ 75,000	$ -	$75,000				
Addition to existing bridge, new footbridge over US340 or multi-purpose path under US 340	$2,000,000	$ -	$ 2,000,000	17.91%	$358,114.57	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Traffic and safety enhancements at US340 and Augustine - City contribution to improve safety at the intersection that results from increased traffic in the area from growth.	$1,000,000	$ -	$ 1,000,000	17.91%	$179,057.28	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Augustine Avenue Trail. Connect new development on the east side of Augustine Ave. to proposed multi-purpose trail. Includes crosswalks lighting, safety features, etc. - Location East Side Developments	$200,000	$ -	$ 200,000	17.91%	$35,811.46	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Westend Gateway, WV 51 / Summit Point Road / W Washington Street - City contribution to facilitate road utility, and pedestrian improvements.	$4,000,000	$ -	$ 4,000,000	17.91%	$716,229.13	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Charles Street Improvements - N. Charles Street, Implement plan for community event space/infrastructure improvements that will enhance community engagement for new residents	$500,000	$ -	$ 500,000	17.91%	$89,528.64	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Offsetting Revenues							
Transportation Facilities Subtotal	**$ 7,775,000**		**$ 7,775,000**				
Total	**$ 15,275,000**	**$ -**	**$ 15,275,000**				

Appendix B-2
DEVELOPER FEES
CITY OF CHARLES TOWN WV
PUBLIC FACILITIES NEEDS LIST THROUGH 2040
(Medium Capital Cost Improvement Scenario)

Facility Name	Total Cost for Facility	Off-setting Revenues	Net Cost to City	Percent of Cost Allocated to New Development	Cost Allocated to New Development	Policy Background or Objective
Fire						
Equipment and Facility upgrade due to growth for both fire companies - Independent and Citizens Fire Companies	**$500,000**		$ 500,000	19.33%	$96,652	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Fire Facilities Subtotal	**$ 500,000**	**$ -**	**$ 500,000**			
Police						
Vehicles and Equipment	$800,000	$ -	$ 800,000	19.33%	$154,643	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Police Facilities Subtotal	**$ 800,000**	**$ -**	**$ 800,000**			
Municipal Facilities						
Expansion of Police Headquarters - added security features and build out of existing CTUB space to accommodate larger police force	$300,000	$ -	$ 300,000	19.33%	$57,991	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
City Hall Expansion / Renovations - Growing community will require additional space to accommodate staff. 101 W Washington St.	$4,000,000	$ -	$ 4,000,000	19.33%	$773,216	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Maintenance yard and facility - new facility will be needed to house and maintain additional equipment required to serve a larger community - Water Street	$750,000	$ -	$ 750,000	19.33%	$144,978	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Storm Water equipment - Replacement street sweeper to service additional roads / gutters resulting from growth; sweeper will preserve stormwater system by preventing debris from entering - Water Street	$350,000	$ -	$ 350,000	19.33%	$67,656	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Municipal Facilities Subtotal	**$ 5,400,000**	**$ -**	**$ 5,400,000**			
Library Facilities						
Placeholder project - Equipment to accommodate future growth such as the acquisition of books and materials, computer equipment, required replacement of facilities and capital improvements,	$200,000	$ -	$ 200,000	19.83%	$39,665	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Library Facilities Subtotal	**$ 200,000**	**$ -**	**$200,000**			

Parks and Recreation							
Expansion of Pool to accommodate growth - Jefferson Memorial Park	$700,000	$ -	$ 700,000	19.83%	$138,828	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Acquisition of parkland and amenities to accommodate future growth - includes tennis courts, pickle ball courts, play fields, play equipment	$500,000	$ -	$ 500,000	19.83%	$99,163	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Walking Bridges that connect existing parks on the west end of town. Evitts Run Park and Happy Retreat	$400,000	$ -	$ 400,000	19.83%	$79,330	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Offsetting Revenues							
Parks Facilities Subtotal	**$ 1,600,000**	**$ -**	**$1,600,000**				
Transportation							
Feasibility Study to examine options for connecting Wards 2 and 4 to downtown	$ 75,000	$ -	$75,000				
Addition to existing bridge, new footbridge over US340 or multi-purpose path under US 340	$2,000,000	$ -	$ 2,000,000	17.91%	$358,114.57	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Traffic and safety enhancements at US340 and Augustine - City contribution to improve safety at the intersection that results from increased traffic in the area from growth.	$1,000,000	$ -	$ 1,000,000	17.91%	$179,057.28	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Augustine Avenue Trail. Connect new development on the east side of Augustine Ave. to proposed multi-purpose trail. Includes crosswalks lighting, safety features, etc. - Location East Side Developments	$200,000	$ -	$ 200,000	17.91%	$35,811.46	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Westend Gateway, WV 51 / Summit Point Road / W Washington Street - City contribution to facilitate road utility, and pedestrian improvements.	$5,000,000	$ -	$ 5,000,000	17.91%	$895,286.41	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Charles Street Improvements - N. Charles Street, Implement plan for community event space/infrastructure improvements that will enhance community engagement for new residents	$500,000	$ -	$ 500,000	17.91%	$89,528.64	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Offsetting Revenues							
Transportation Facilities Subtotal	**$ 8,775,000**		**$ 8,775,000**				
Total	**$ 17,275,000**	**$ -**	**$ 17,275,000**				

Appendix B-3
DEVELOPER FEES
CITY OF CHARLES TOWN WV
PUBLIC FACILITIES NEEDS LIST THROUGH 2040
(High Capital Cost Improvement Scenario)

Facility Name	Total Cost for Facility	Off-setting Revenues	Net Cost to City	Percent of Cost Allocated to New Development	Cost Allocated to New Development	Policy Background or Objective
Fire						
Equipment and Facility upgrade due to growth for both fire companies - Independent and Citizens Fire Companies	**$500,000**		$ 500,000	19.33%	$96,652	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Fire Facilities Subtotal	**$ 500,000**	**$ -**	**$ 500,000**			
Police						
Vehicles and Equipment	$800,000	$ -	$ 800,000	19.33%	$154,643	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Police Facilities Subtotal	**$ 800,000**	**$ -**	**$ 800,000**			
Municipal Facilities						
Expansion of Police Headquarters - added security features and build out of existing CTUB space to accommodate larger police force	$300,000	$ -	$ 300,000	19.33%	$57,991	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
City Hall Expansion / Renovations - Growing community will require additional space to accommodate staff. 101 W Washington St.	$5,000,000	$ -	$ 5,000,000	19.33%	$966,520	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Maintenance yard and facility - new facility will be needed to house and maintain additional equipment required to serve a larger community - Water Street	$750,000	$ -	$ 750,000	19.33%	$144,978	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Storm Water equipment - Replacement street sweeper to service additional roads / gutters resulting from growth; sweeper will preserve stormwater system by preventing debris from entering - Water Street	$350,000	$ -	$ 350,000	19.33%	$67,656	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Municipal Facilities Subtotal	**$ 6,400,000**	**$ -**	**$ 6,400,000**			
Library Facilities						
Placeholder project - Equipment to accommodate future growth such as the acquisition of books and materials, computer equipment, required replacement of facilities and capital improvements,	$200,000	$ -	$ 200,000	19.83%	$39,665	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21
Offsetting Revenues						
Library Facilities Subtotal	**$ 200,000**	**$ -**	**$200,000**			

Parks and Recreation							
Expansion of Pool to accommodate growth - Jefferson Memorial Park	$700,000	$ -	$ 700,000	19.83%	$138,828	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Acquisition of parkland and amenities to accommodate future growth - includes tennis courts, pickle ball courts, play fields, play equipment	$500,000	$ -	$ 500,000	19.83%	$99,163	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Walking Bridges that connect existing parks on the west end of town. Evitts Run Park and Happy Retreat	$400,000	$ -	$ 400,000	19.83%	$79,330	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Offsetting Revenues							
Parks Facilities Subtotal	**$ 1,600,000**	**$ -**	**$1,600,000**				
Transportation							
Feasibility Study to examine options for connecting Wards 2 and 4 to downtown	$ 75,000	$ -	$75,000				
Addition to existing bridge, new footbridge over US340 or multi-purpose path under US 340	$2,000,000	$ -	$ 2,000,000	17.91%	$358,114.57	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Traffic and safety enhancements at US340 and Augustine - City contribution to improve safety at the intersection that results from increased traffic in the area from growth.	$1,000,000	$ -	$ 1,000,000	17.91%	$179,057.28	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Augustine Avenue Trail. Connect new development on the east side of Augustine Ave. to proposed multi-purpose trail. Includes crosswalks lighting, safety features, etc. - Location East Side Developments	$200,000	$ -	$ 200,000	17.91%	$35,811.46	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Westend Gateway, WV 51 / Summit Point Road / W Washington Street - City contribution to facilitate road utility, and pedestrian improvements.	$6,000,000	$ -	$ 6,000,000	17.91%	$1,074,343.70	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Charles Street Improvements - N. Charles Street, Implement plan for community event space/infrastructure improvements that will enhance community engagement for new residents	$500,000	$ -	$ 500,000	17.91%	$89,528.64	Growth Related Capital Improvement Projects - Developer Fee Analysis as of 11/30/21	
Offsetting Revenues							
Transportation Facilities Subtotal	**$ 9,775,000**		**$ 9,775,000**				
Total	**$ 19,275,000**	**$ -**	**$ 19,275,000**				

dta

www.FinanceDTA.com

614 NORTH CAROLINA BLVD. UNIT 202
RALEIGH, NC 27603
PHONE: (800) 969-4DTA

Public Finance
Public-Private Partnerships
Development Economics
Clean Energy Bonds

Proffered/Conditions of Annexation Fees and Dedications to the City, by Subdivision – Oct. 14, 2026

1. **Augustine Manor** (Vinton Hayes) $2,500
   A. $2,500 per residential unit
   B. Dedicate to the City (prior to the issuance of the 291st residential building permit):
      i. A full-sized soccer field
      ii. Two pickle ball courts

2. **Avalon/Farview**
   A. $3,494 per residential unit
   B. $2,958 per thousand square feet of commercial space
   C. A trail system consistent with the Comprehensive Plan

3. **Huntfield**
   A. $2448.00 per dwelling unit.
   B. Dedicate to the City up to 10 acres of improved (utilities and hard surface road frontage) for municipal facilities.
   C. Dedicate to the Board of Education up to 17 acres of land.
   D. To build an 8ft. wide hiker/biker trail in accordance with the Huntfield Master Plan.

4. **Norborne Glebe**
   A. $500.00 per dwelling unit.
   B. Up to 66 acres of land (was turned into Willingham Knolls Park)

5. **Prospect Place**
   A. $2,722 for every single family/townhome unit
   B. $925 for every multifamily rental apartment unit.

6. **Stone Spring**
   A. Each new residential unit (except those in a mixed-use structure) shall pay $2,448 per unit. This is subject to review/adjustment every 5 years starting March 27, 2028.
   B. Pay $50,000 to the City for a pedestrian connectivity study for the residents of the 4th Ward (already paid).
   C. Parkland dedication to include vehicular access and parking improvements (not yet dedicated over.)

7. **Washington Place South (Langlet Farm South)**
   A. $948 per residential unit for capital improvement costs and $4,500 for fiscal impacts, per unit. These fees may be adjusted on a bi-annual and inflationary basis. Workforce Housing Units are exempt from these fees.
   B. Shall construct and dedicate three park areas to the City.

KeyCite Yellow Flag
Proposed Legislation

West's Annotated Code of West Virginia
Chapter 8. Municipal Corporations
Article 13. Taxation and Finance
Part III. Special Charges for Municipal Services

W. Va. Code, § 8-13-13

§ 8-13-13. Special charges for municipal services

Effective: July 9, 2025
Currentness

(a) Notwithstanding any charter provisions to the contrary, a municipality which furnishes any essential or special municipal service, including, but not limited to, police and fire protection, parking facilities on the streets or otherwise, parks and recreational facilities, street cleaning, street lighting, street maintenance and improvement, sewerage and sewage disposal, and the collection and disposal of garbage, refuse, waste, ashes, trash, and any other similar matter, has plenary power and authority, subject to the limitations set forth in subsection (b) of this section, to provide by ordinance for the installation, continuance, maintenance, or improvement of the service, to make reasonable regulations of the service, and to impose by ordinance upon the users of the service reasonable rates, fees, and charges to be collected in the manner specified in the ordinance.

(b)(1) No new fire protection fee or charge, effective on or after June 30, 2024, may be imposed pursuant to this section on a person or business situated outside of the municipality's boundaries in a county that has imposed a county fire service fee pursuant to § 7-17-12 of this code unless the municipality has entered into an intergovernmental agreement, which complies with the limitations set forth in subdivision (2) of this subsection, with the county commission having jurisdiction over any such person or business.

(2) The intergovernmental agreement referenced in subdivision (1) of this subsection must include, but is not limited to, the following terms:

(A) The municipality's fire protection fees and charges shall be limited to those persons and businesses located within first due areas covered by fire protection services sourced out of the municipality; and

(B) The municipality's fire protection fees and charges shall be the same for all persons and businesses located within and outside of the municipality's boundaries; and

(C) Under no circumstances may any person or business be required to pay both a municipal fire protection fee or charge pursuant to this section and a county fire service fee pursuant to § 7-17-12 of this code, except for the pro-rata reconciliation during the first year after passage as set forth in paragraph (D) of this subdivision; and

 © 2026 Thomson Reuters. No claim to original U.S. Government Works.

(D) If any persons and businesses located within first due areas have paid their county fire service fee during the first year after the effective date of the amendments to this section enacted during the 2025 Regular Legislative Session, then (i) any municipality's fire protection fees and charges imposed by the municipality shall be limited to the difference, if any, between the county's fire service fee and the municipality's fire protection fees and charges within its municipal boundaries; and (ii) the county shall transfer its fire service fee revenues received from all persons and businesses located within first due areas that are covered by the intergovernmental agreement to the municipality; and

(E) After the first year following the effective date of the amendments to this section enacted during the 2025 Regular Legislative Session, persons and businesses located within first due areas covered by the intergovernmental agreement between the county commission and the municipality shall be subject only to the same municipal fire protection fees and charges which the municipality charges all other residents and businesses within its municipal boundaries.

(F) The intergovernmental agreement shall expire five years after the agreement becomes effective. The agreement may be renewed for successive additional terms of no more than five years each.

(3) Notwithstanding subdivisions (1) and (2) of this subsection, any municipality may increase or decrease, in accordance with this section, a fire protection fee or charge that was in effect prior to June 30, 2024, so long as such increase or decrease is uniform for all persons and businesses that are subject to the municipality's fire protection fees and charges, whether by residency within municipal boundaries or by being subject controlling intergovernmental agreement.

(c) Any sewerage and sewage disposal service and any service incident to the collection and disposal of garbage, refuse, waste, ashes, trash, and any other similar matter is subject to the provisions of Chapter 24 of this code.

(d) A municipality may not have a lien on any property as security for payments due under subsection (a) of this section except as provided in subsection (e) of this section.

(e) A municipality may enact an ordinance, pursuant to this section, permitting it to file a lien on real property located within the municipal corporate limits for unpaid and delinquent fire, police, or street fees. The ordinance shall provide an administrative procedure for the municipality's assessment and collection of the fees. The administrative procedure shall require that, before any lien is filed, the municipality will give notice to the property owner, by certified mail, return receipt requested, that the municipality will file the lien unless the delinquency is paid by a date stated in the notice, which shall be no less than 90 days from the date the notice is mailed. The administrative procedure shall include the right to appeal to the circuit court of the county in which the real property is located. The circuit court shall consider the appeal under its general authority, including but not limited to § 51-2-2(f) of this code.

(f) Notwithstanding the provisions of § 8-11-4 of this code, any ordinance enacted or substantially amended under the provisions of this section shall be published as a Class II legal advertisement in compliance with the provisions of § 59-3-1 *et seq.* of this code. The publication area for the publication is the municipality.

(g) If 30 percent of the qualified voters of the municipality, by petition duly signed by them in their own handwriting and filed with the recorder of the municipality within 45 days after the expiration of the publication, protest against the ordinance as enacted or amended, the ordinance may not become effective until it is ratified by a majority of the legal votes cast by the

 © 2026 Thomson Reuters. No claim to original U.S. Government Works.

qualified voters of the municipality at a regular municipal election or special municipal election, as the governing body directs. Voting may not take place until after notice of the submission is given by publication as provided in subsection (f) of this section.

(h) The powers and authority granted to municipalities and to the governing bodies of municipalities in this section are in addition and supplemental to the powers and authority named in any charters of the municipalities.

(i) Notwithstanding any other provisions of this section, if rates, fees, and charges provided in this section are imposed by the governing body of a municipality for the purpose of replacing, and in amounts approximately sufficient to replace in its general fund amounts appropriated to be paid from ad valorem taxes upon property within the municipality, pursuant to an election duly called and held under the Constitution and laws of the state to authorize the issuance and sale of the municipality's general obligation bonds for public improvement purposes, the call for the election shall state that the governing body of the municipality proposes to impose rates, fees, and charges in specified amounts under this section for the use of one or more of the services specified in subsection (a) of this section, which shall be related to the public improvement proposed to be made with the proceeds of the bonds, no notice, publication of notice, or referendum, or election or other condition or prerequisite to the imposition of the rates, fees, and charges shall be required or necessary other than the legal requirements for issuance and sale of the general obligation bonds.

(j) Payments for rates, fees, and charges due under this section that are postmarked after the due date by which they are owed shall be considered late and may be subject to late fees or penalties: *Provided*, That payments that are received by the municipality after the due date, but that were postmarked on or before the due date shall be considered to be on time and shall not be assessed any late fees or penalties.

Credits

Acts 1921, c. 111, §§ 1, 2; Acts 1933, Ex. Sess., c. 27; Acts 1937, c. 56; Acts 1951, c. 134; Acts 1955, c. 119; Acts 1959, c. 115; Acts 1961, c. 99; Acts 1967, c. 105; Acts 1969, c. 86; Acts 1971, c. 99; Acts 2009, c. 161, eff. July 10, 2009; Acts 2022, c. 281, eff. June 10, 2022; Acts 2024, 2nd Ex. Sess., c. 33, eff. Oct. 8, 2024; Acts 2025, c. 186, eff. July 9, 2025.

Formerly Code 1923, c. 47, § 62.

Notes of Decisions (63)

W. Va. Code, § 8-13-13, WV ST § 8-13-13
Current with legislation of the 2026 Regular Session. Some statute sections may be more current, see credits for details.

End of Document

© 2026 Thomson Reuters. No claim to original U.S. Government Works.

ARTICLE IV. CITY SERVICES FEE

Sec. 13-60. Legislative findings.

(a) The city council of the city finds that W. Va. Code § 8-13-13 provides that every municipality which furnishes any essential or special municipal service has the plenary power and authority to adopt by ordinance for the installation, continuance, maintenance, or improvement of such services to make reasonable regulations with respect thereto and to impose by ordinance upon the users of such services reasonable rates, fees and charges to be collected in the manner prescribed in the ordinance.

(b) The city council of the city finds that the city provides to all individuals within its borders certain services, whether they are residents or visitors.

(c) The city council of the city finds that such municipal services include police protection; general government administrative services; governmental buildings and facilities; parking facilities on streets and otherwise; parks and recreational facilities; street cleaning; street lighting; street maintenance and improvement; sewerage collection; and disposal of garbage, refuse, waste, ashes, trash; and any other similar matter.

(d) The city council of the city finds that such services are within the authority and responsibility of the municipal government of the city as provided under the general laws of the state.

(e) The city council of the city finds that residential and commercial development in the city and attendant increases in population requires additional essential municipal services and improvements to existing municipal services so all citizens of the city will have fair and equitable access to essential municipal services.

(f) The city council of the city finds that all new residential and commercial building permit applicants, who use, enjoy and benefit from these services, should bear the equitable share of the costs thereof.

(g) The city council of the city finds that the imposition of the city services fee established herein is a reasonable system of distributing the costs of such services to all new residential and commercial building permit applicants.

(h) The city council of the city finds that it is in the best interest of the citizens of the city and users of city services to enact this section to impose a city services fee.

(i) The city council of the city finds that a report commissioned by the city and prepared by URS Corporation dated November 2005, titled "Development Impact Analysis Fiscal Model City of Ranson, West Virginia" which "details the analysis of fiscal impacts associated with proposed residential and commercial development in the City of Ranson, West Virginia" is a reasonable basis to establish the city services fee under this section. The fiscal model suggests that the city set a city services fee between $1,409.00 to $1,904.00 per each residential unit.

(Ord. No. 189, 10-21-08)

Sec. 13-61. Imposition of fee; rate.

There is hereby imposed a city services fee of $1,000.00 upon each new residential building permit issued in the city and a fee of $0.75 per square foot of commercial space for each new commercial building permit issued by the city. The fee shall be collected prior to building permit issuance for all residential and commercial development

in the city and represents 52 percent of the total recommended by the URS report. The fee imposed by this section is in addition to all other fees imposed by the city.

(Ord. No. 189, 10-21-08)

Sec. 13-62. Declaration as to conduct evidencing the use of a municipal service.

The city council of the city declares that the pulling of a building permit within the city is legal and valid proof of the use of one or more municipal services sufficient to assess and collect a city service fee from the individual engaging in the activity stated. As such structure and its occupants, customers, visitors, residents, lessees, and tenants will utilize the essential municipal services set out in this Code.

(Ord. No. 189, 10-21-08)

Sec. 13-63. Dedication of revenues.

All revenues generated by the city services fee imposed herein are hereby dedicated to and shall be exclusively utilized for police protection; parking facilities on streets and otherwise; parks and recreational facilities; street cleaning; street lighting; street maintenance and improvement and public works projects related thereto; sewerage collection; disposal of garbage, refuse, waste, ashes and trash; and any costs related to the imposition of processing this fee.

(Ord. No. 189, 10-21-08)

Sec. 13-64. Enforcement.

The city manager or his designee is charged with the administration and enforcement of this section and may, among other remedies, withhold the issuance of the building permit until the city services fee is paid in full or institute appropriate legal proceedings in the name of the city against any person or entity who fails or refuses to pay the city services fee imposed herein.

(Ord. No. 189, 10-21-08)

Sec. 13-65. Protest; administrative decision; appeal.

(a) Any person or entity who has paid the city services fee imposed by this section shall file a claim for refund no later than 30 days after the fee is paid over to the city by written notice of such claim with the city manager setting forth the with particularity all objections thereto. The burden of proof shall be upon the aggrieved party to show that the fee was paid and is incorrect and contrary to law, in whole or in part. The city manager or his designee shall review the refund claim and provide for any necessary hearing, render a decision on the claim and forthwith either notify the protesting party of such decision in writing or direct that a refund be issued, all within a reasonable time. Said decision shall be issued by certified mail, return receipt requested.

(b) If aggrieved by the decision of the city manager, the protesting party may appeal the decision of the city manager to the county circuit court within 30 days after service of the city manager's decision.

    (1) The appeal shall be taken by the filing of a petition and notice, which petition and notice shall be served upon or accepted by the city manager as an original notice. When the petition and notice is so served it shall, with the return or acceptance thereon, be filed in the office of the clerk of the county

circuit court and docketed as other cases, with the aggrieved party as plaintiff and the city as defendant.

(2) The filing of the appeal shall not stay the collection of the fee unless the plaintiff shall file with such clerk a bond for the use of the defendant, with sureties approved by the clerk of the circuit court of the county, the penalty of the bond to be not less than the total amount of the fee, and accumulated penalties to the date of the appeal, and conditioned that the plaintiff shall perform the orders of the county circuit court; provided, that the judge of the county circuit court may stay the collection of the fee, and accumulated penalties without the requirement of a bond, upon a proper showing by the plaintiff that the properties of the plaintiff are sufficient to secure performance of the county circuit court's orders or that the ends of justice will be served thereby.

(3) The county circuit court shall hear the appeal and determine anew all questions submitted to it on appeal from the decision of the city manager. In such appeal a certified copy of the city's fee assessment shall be admissible and shall constitute prima facie evidence of the fee due under the provisions of this section.

(c) The administrative remedies set forth in this section are exclusive. Failure to timely file a refund claim in accordance with this section shall preclude any right to refund with respect to any fee paid to the city prior to the claim. If no appeal is taken pursuant to this section within 30 days after service of the city manager's decision, said decision shall become final and conclusive and not subject to administrative or judicial review. The amount of the fee and accumulated penalties, if any, due the city under such decision shall be due and payable on the day following the date upon which such decision becomes final.

(Ord. No. 189, 10-21-08)

Sec. 13-66. Effective date.

The imposition of the city services fee shall become effective on November 10, 2008, unless a petition is submitted in accordance with the provisions of W. Va. Code § 8-13-13, and shall remain in full force and effect until such time as rescinded by further ordinance of council. The city services fee shall not apply to any building permit wherein the application for said building permit was filed with the city on or before November 9, 2008.

(Ord. No. 189, 10-21-08)

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2048: FY2027 General Fund Budget Revision #3

ATTACHMENTS:

- FY 2027 GF Revision #3.pdf

FY 2026-2027
General Fund Budget

(Includes 2.7% COLA & 2.5% Merit Salary Increases)

ACCOUNT	FY 2027 APPROVED BUDGET	REVISION #1	REVISION #2	REVISION #3	CURRENT BUDGET	FY 2027 YTD ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES AND EXPLANATIONS	REVISION #1 NOTES	REVISION #2 & #3 NOTES
REVENUES											
300-050 Unassigned Fund Balance (Carryover)	650,000	1,558,120			2,208,120	2,208,120	(0)	100%	Estimated carryover balance for fiscal year ending 2026	Increased carryover to reflect actual balance as of 6/30/26	
301-010 Taxes - Ad Valorem	2,021,996				2,021,996	1,130,485	891,511	56%	Property taxes		
301-060 Supplemental Taxes	40,000				40,000	17,637	22,363	44%	Property taxes owed from previous years, but paid in the current fiscal year		
302-000 Interest and Penalty	10,000				10,000	4,185	5,815	42%	Interest and penalties on property taxes		
303-000 Gas & Oil Severance Tax	20,000				20,000	-	20,000	0%	5% severance tax on gross receipts at the well head of oil and natural gas		
304-000 Utility Tax (2%)	300,000				300,000	53,973	246,027	18%	Public utility services taxes		
305-000 Business & Occupation (B&O) Tax	2,056,946				2,056,946	1,089,131	967,815	53%	B&O taxes as well as estimated receipts from HDL collections service efforts		
306-000 Liquor Tax	25,000				25,000	8,176	16,824	33%	Tax on purchase of intoxicating liquors		
307-000 Animal Control Tax	1,600				1,600	1,129	471	71%	This is donated back to the county each year under Dog Warden		
308-000 Hotel/Motel Tax	175,000				175,000	44,098	130,902	25%	3 traditional hotels (Rodeway Inn, Days Inn, Carriage Inn) and 5 independent rental companies (Homeaway.com, Expedia, Airbnb, Hotel Tonight, Evolve Vacation Rental Network)		
320-000 Court Costs, Fees & Charges	260,000				260,000	54,286	205,714	21%			
321-000 Parking Violation Penalties	40,000				40,000	7,700	32,300	19%			
325-000 Business License Revenue	45,000				45,000	14,055	30,945	31%			
326-000 Building Permit Fees	750,000				750,000	185,089	564,911	25%	Building activity increasing/expected to remain strong through FY2027 with new development projects on the horizon and increases in permit fee structure		
328-000 Franchise Tax	65,000				65,000	13,184	51,816	20%	Cable Franchise		
329-000 Rental Registration Fees	1,000				1,000	-	1,000	0%			
330-000 International Registration Plan (IRP) Fees	70,000				70,000	17,177	52,823	25%	The International Registration Plan is an agreement for the registration of commercial motor vehicles that travel in the United States. It is designed to distribute apportioned taxes (registration fees) depending on the mileage driven in the participating jurisdictions		
339-000 Emergency Service Fee	1,700				1,700	412	1,288	24%	Revenue from utility bills for EMS (5 cents)		
340-000 Parks & Rec Fee	1,700				1,700	412	1,288	24%	Revenue from utility bills for parks and recreation (5 cents)		
342-000 Parking Meter Revenues	50,000				50,000	16,401	33,599	33%	Revenue from parking meters and parking permits including ParkMobile ap		
345-000 Rents & Concessions	60,000				60,000	17,190	42,810	29%	CTUB rental of 661 space ($30,000); CWH tenant rental ($30,000) Rouss Hall tenant rental ($5000)		
353-000 Zoning Fee	20,000				20,000	48,332	(28,332)	242%	Planning Commission zoning application fees		
355-000 Street Improvement Fee	150,000				150,000	32,148	117,852	21%	Revenue from utility bills for street improvements ($4 per month)		
365-040 Federal Government Grants	41,700	189,000			230,700	-	230,700	0%	DOJ/COPS grant for additional police officer. $125,000 across 3 years	Remaining HUD grant funds from FY 2026	
366-000 State Government Grants	3,000				3,000	-	3,000	0%	Fairs and Festivals grant for WV Fest and Christmas Parade		
367-000 Other Grants					-	-	-		Donations to police department and Tree Board		
369-000 Contributions from Other Funds - Sales Tax ($1,600,000); Housing Rehab ($68,000); Vacant Structures ($24,000); OPIOID ($75,000)	1,767,000				1,767,000	475,000	1,292,000	27%	Ordinance requires sales tax contribution first pays debt first (payments to BC are rent payments in PD and CH budgets to cover BC debt). Quarterly sales tax distributions are averaging $500,000 or $2,000,000 annually. Housing Rehab supports Code Enforcement nuisance properties contracted services. Vacant Structures supports Code Enforcement vacant structures contracted services. OPIOID supports Police social worker services contracted services.		
376-000 Gaming Income	250,000				250,000	56,694	193,306	23%	Gaming receipts average $19K to $23K per month		
379-000 Gain/Loss - Sale of Fixed Assets					-	250	(250)				
380-000 Interest Income (Operating Acct)	25,000				25,000	3,926	21,074	16%	Interest on checking accounts		
381-000 Reimbursements	130,000				130,000	9,282	120,718	7%	SRO reimbursement ($60,000); crossing guards ($40,000); police overtime reimbursements ($10,000); Fuel Refunds ($9600); Pcard Rebate ($6000); Alarm Calls ($2000)		
381-000 Lein Reimbursements					-	-	-				
382-000 Refunds - Overpayments	500				500	19,405	(18,905)	3881%			
386-000 Insurance Claims				100,407	100,407	104,484	(4,077)				Insurance revenue received on a totaled police cruiser recognized in the GF Budget to be transferred to the Capital Fund for purchase of a new vehicle
392-000 Property Rehabilitation	7,500				7,500	100	7,400	1%	Vacant Structures Fees		
387-000 Filing Fees	200				200	-	200	0%	Filing Fees Revenue - Election in FY 2027. 1% of annual salary per person		
397-000 Video Lottery	700,000				700,000	66,419	633,581	9%	Video lottery receipts average $13.4K to $22.2K per week		
399-000 Misc Revenue	7,500				7,500	2,077	5,423	28%	Yard waste stickers and fingerprints		
399-010 Misc Revenue - CC Service Fees						2,719	(2,719)				
399-020 Special Events - WV Fest	15,000				15,000	-	15,000	0%	Vendor registration fees and sponsors for WV Fest		
399-030 Special Events - General	1,000				1,000	125	875	13%	Special activities fees		
399-040 Special Events - CW Hall	15,000				15,000	2,200	12,800	15%	CW Hall public rental fees		
399-070 Special Events - Car Show	7,500				7,500	11,414	(3,914)	152%	Car show registration and sponsors		
TOTAL REVENUES	**9,785,842**	**1,747,120**	**-**	**100,407**	**11,633,368**	**5,717,414**	**5,915,954**	49%			

ACCOUNT	FY 2027 APPROVED BUDGET	REVISION #1	REVISION #2	REVISION #3	CURRENT BUDGET	FY 2027 YTD ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES AND EXPLANATIONS	REVISION #1 NOTES	REVISION #2 & #3 NOTES
EXPENSES											
ECONOMIC DEVELOPMENT - 402											
402-103 Salaries	83,000				83,000	21,271	61,729	26%	Business Development /Downtown Coordinator salary plus 2.5% merit and holiday supplement		
402-104 FICA	6,600				6,600	1,612	4,988	24%	FICA @ 7.65%		
402-105 Group Insurance	10,000	1,000			11,000	2,519	8,481	23%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
402-106 Retirement	7,000				7,000	1,914	5,086	27%	PERS I & II Employer Contribution 8%		
402-109 OPEB	250	400			650	150	500	23%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
402-110 Fringe Benefits	1,800				1,800	425	1,375	24%	457(b) Deferred Compensation Employer Contribution (3%)		
402-211 Telephone	500				500	67	433	13%	Cell phone		
402-214 Travel	3,000				3,000	157	2,843	5%	2 National Conferences; airfare, lodging, per-diem		
402-220 Advertising/Legal Publications	500				500	-	500	0%			
402-221 Training & Education	2,500				2,500	690	1,810	28%	Economic Development Certifications		
402-222 Dues & Subscriptions	3,100				3,100	224	2,876	7%	IEDC Membership (400), Music Subscription ($250); QR Code Subscriptions ($180); Map Ap Subscription ($2100); Imagine AI ($100)		
402-223 Professional Services	3,000				3,000	-	3,000	0%	Engineering services, appraisals, renderings		
402-341 Departmental Supplies	5,000				5,000	3,187	1,813	64%	Promotional items for events and City marketing and other departmental supplies. Welcome bags for new residents ($1,000)		
TOTAL ECONOMIC DEVELOPMENT	**126,250**	**1,400**	-	-	**127,650**	**32,217**	**95,433**	25%			
MAYOR'S OFFICE - 409											
409-101 Salary	12,500				12,500	3,000	9,500	24%	Mayor's Salary		
409-104 FICA Tax Expense	1,000				1,000	229	771	23%	FICA @ 7.65%		
409-211 Telephone	600				600	95	505	16%	Cell phone		
409-214 Travel Expense	2,000				2,000	596	1,404	30%	WV Municipal League conference & other trainings		
409-221 Training & Education	1,000				1,000	-	1,000	0%	WV Municipal League conference & other trainings		
409-341 Departmental Supplies	500	2,500			3,000	2,475	526	82%	Ceremonial Keys to the City and Coins	Allowance for purchase of ceremonial coins	
409-568 Community Contributions	2,000				2,000	-	2,000	0%			
TOTAL MAYOR'S OFFICE	**19,600**	**2,500**	-	-	**22,100**	**6,395**	**15,705**	29%			
COUNCIL - 410											
410-101 Salaries	40,000				40,000	10,000	30,000	25%	Eight Council Members at $5,000 annual salary		
410-104 FICA Tax Expense	3,100				3,100	765	2,335	25%	FICA @ 7.65%		
410-214 Travel Expense	5,000				5,000	1,813	3,187	36%	WV Municipal League conference & other trainings		
410-221 Training & Education	3,000	1,100			4,100	1,103	2,997	27%	WV Municipal League Conference Registration ($450 per registration) & other trainings	Allowance for participation in Leadership Jefferson program	
410-341 Departmental Supplies	1,000				1,000	-	1,000	0%			
TOTAL COUNCIL	**52,100**	**1,100**	-	-	**53,200**	**13,681**	**39,519**	26%			
CITY MANAGER - 412											
412-103 Salaries	205,000				205,000	87,033	117,967	42%			
412-104 FICA Tax Expense	18,000				18,000	6,696	11,304	37%	FICA Tax @ 7.65%		
412-105 Group Insurance	23,000				23,000	2,572	20,428	11%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)		
412-106 Retirement	18,000				18,000	3,445	14,555	19%	PERS I & II Employer Contribution 8%		
412-108 Overtime	2,500				2,500	494	2,006	20%			
412-109 OPEB	250	400			650	50	600	8%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
412-110 Fringe Benefits	6,200				6,200	1,048	5,152	17%	457(b) Deferred Compensation Employer Contribution (3%)		
412-211 Telephone	550				550	-	550	0%	Cell phone service		
412-214 Travel Expense	1,500				1,500	-	1,500	0%	WVML Trip, City Clerk Election Training		
412-220 Advertising	1,500				1,500	-	1,500	0%	Job advertising		
412-221 Training & Education	1,000				1,000	300	700	30%	WVML Conference, City Clerk Election Training		
412-222 Dues & Subscriptions	1,000				1,000	124	876	12%	ICMA and WVML Fees.		
412-223 Professional Services	500		50,000		50,500	-	50,500	0%	Background checks for City Manager candidates.		Allowance for City Manager recruiting
412-341 Departmental Supplies	750				750	22	728	3%	Office Supplies		
TOTAL CITY MANAGER	**279,750**	**400**	**50,000**	**-**	**330,150**	**101,784**	**228,366**	31%			
TREASURER - 413											
413-103 Salaries	275,000			(3,000)	272,000	59,184	212,816	22%	Director of Finance, Accounting Clerk I, Accounting Clerk II, Accounting Clerk III salaries, 2.5% merit, and holiday supplements.		Transfer to Treasurer Overtime
413-104 FICA Tax Expense	23,000				23,000	4,790	18,210	21%	FICA Tax @ 7.65%		
413-105 Group Insurance	40,000				40,000	8,018	31,982	20%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)		
413-106 Retirement	25,000				25,000	4,836	20,164	19%	PERS I & II Employer Contribution 8%		
413-108 Overtime	3,700			3,000	6,700	3,822	2,878	57%			Increase due to vacancy
413-109 OPEB	750	1,100			1,850	401	1,449	22%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
413-110 Fringe Benefits	7,100				7,100	1,732	5,368	24%	457(b) Deferred Compensation Employer Contribution (3%)		
413-214 Travel Expense	1,500				1,500	-	1,500	0%	Biannual Director & Acct. Clerk III - WV Government Finance Officers Association Training		
413-218 Postage	2,000				2,000	-	2,000	0%	Certified Mailings for collections communications		
413-220 Advertising/Legal Pubs	2,500				2,500	165	2,335	7%	Financial statement publication $625, Levy Estimate $425 and job advertising.		
413-221 Training & Education	1,000				1,000	-	1,000	0%	GFOA bi-annual trainings.		
413-222 Dues & Subscriptions	1,000				1,000	975	25	98%	GFOA memberships for Finance Director and Accounting Clerk III		
413-223 Professional Services	2,500				2,500	2,100	400	84%	Police pension annual report ($2100) Background Checks for New Hires ($100)		
413-224 Audit Costs	50,000	22,000			72,000	18,063	53,937	25%	Perry & Associates and J.C. Kunkle FY26 Compilation and Preparation of Audit	Allowance for FY 2025 audit expenses	
413-230 Contracted Services - B&O Collections	20,000				20,000	3,036	16,964	15%	Fees for collection services		
413-238 Refunds	50,000				50,000	742	49,258	1%			
413-341 Departmental Supplies	1,500				1,500	33	1,467	2%	Office Supplies		
413-353 Computer Software/Tech		45,000			45,000	40,555	4,445	90%	Tyler Technologies - Incode Annual License Fee ($35,000 for ERPRO 10 & $10,000 for ERPRO 9)		
TOTAL TREASURER	**506,550**	**68,100**	-	-	**574,650**	**148,453**	**426,197**	26%			
COURT CLERK - 415											
415-103 Salaries	72,000				72,000	18,597	53,403	26%	Court Clerk Salary, 2.5% merit, and holiday supplement		
415-104 FICA	5,900				5,900	1,400	4,500	24%	FICA Tax @ 7.65%		
415-105 Group Insurance	21,000				21,000	5,171	15,829	25%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)		
415-106 Retirement	6,000				6,000	1,692	4,308	28%	PERS I & II Employer Contribution 8%		
415-108 Overtime	1,000				1,000	198	802	20%			
415-109 OPEB	250	400			650	150	500	23%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
415-110 Fringe Benefits	2,300				2,300	552	1,748	24%	457(b) Deferred Compensation Employer Contribution (3%)		
415-214 Travel	500				500	-	500	0%	Court Clerk training		
415-218 Postage	500				500	-	500	0%	Certified mailings for court communications		
415-220 Advertising/Legal Publications					-	-	-				
415-221 Training & Education	750				750	-	750	0%	WVML training and Election training.		
415-230 Contracted Services	25				25	-	25	0%	Flu shot		
415-238 Refunds	1,000				1,000	162	838	16%			
415-341 Departmental Supplies	750				750	31	719	4%	Ink cartridges, paper stock		
TOTAL COURT CLERK	**111,975**	**400**	-	-	**112,375**	**27,954**	**84,421**	25%			

ACCOUNT	FY 2027 APPROVED BUDGET	REVISION #1	REVISION #2	REVISION #3	CURRENT BUDGET	FY 2027 YTD ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES AND EXPLANATIONS	REVISION #1 NOTES	REVISION #2 & #3 NOTES
POLICE JUDGES - 416											
416-103 Salaries	44,000			(500)	43,500	9,000	34,500	21%	Two Municipal Court judges ($6000); three magistrates ($18,000); two prosecuting attorneys($13,000); extra $2000 for special judge, and holiday supplements ($1750).		Transfer to Police Judges Uniforms
416-104 FICA	3,600				3,600	689	2,912	19%	FICA Tax @ 7.65%		
416-214 Travel	500				500	-	500	0%	WV State mandated annual training for magistrates & judges		
416-221 Training & Education	1,000				1,000	-	1,000	0%	WV State mandated annual training for magistrates & judges		
416-223 Professional Services	1,000				1,000	280	720	28%	Fees for translator.		
416-345 Uniforms				500	500	-	500	0%			Allowance for purchase of magistrate shirts
TOTAL POLICE JUDGES	**50,100**	**-**	**-**	**-**	**50,100**	**9,969**	**40,132**	20%			
CITY ATTORNEY - 417											
417-103 Salaries	170,000				170,000	44,323	125,677	26%	Attorney salary plus 2.5% merit and holiday supplement		
417-104 FICA	13,600				13,600	3,389	10,211	25%	FICA @ 7.65%		
417-105 Group Insurance	1,700	300			2,000	598	1,402	30%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
417-106 Retirement	15,000				15,000	3,989	11,011	27%	PERS I & II Employer Contribution 8%		
417-109 OPEB	-				-	-	-		RHBT Insurance		
417-110 Fringe Benefits	5,500				5,500	1,329	4,171	24%	457(b) Deferred Compensation Employer Contribution (3%)		
417-211 Telephone	250				250	38	212	15%	Cell phone service		
417-214 Travel	2,000				2,000	548	1,452	27%	Travel allowance for WVML and various trainings.		
417-221 Training & Education	2,000				2,000	-	2,000	0%	WVML and other CLE registrations.		
417-222 Dues & Subscriptions	6,000				6,000	1,343	4,657	22%	Bar license and West Law legal research database subscription. IMLA membership.		
417-223 Professional Services	50,000				50,000	-	50,000	0%	Cost for outside legal council		
417-341 Departmental Supplies	750				750	56	695	7%	Office supplies		
TOTAL CITY ATTORNEY	**266,800**	**300**	**-**	**-**	**267,100**	**55,614**	**211,486**	21%			
ENFORCEMENT AGENCY - 425											
425-103 Salaries	65,000				65,000	17,078	47,922	26%	Code Enforcement Officer salary, 2.5% merit, holiday supplement., and clothing allowance		
425-104 FICA	5,200				5,200	1,291	3,909	25%	FICA @ 7.65% of Salary		
425-1.05 Group Insurance	10,000	1,000			11,000	2,466	8,534	22%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
425-106 Retirement	5,500				5,500	1,496	4,004	27%	PERS I & II Employer Contribution 8%		
425-109 OPEB	250	400			650	150	500	23%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
425-110 Fringe Benefits	2,200				2,200	498	1,702	23%	457(b) Deferred Compensation Employer Contribution (3%)		
425-211 Telephone	500				500	38	462	8%	Cell phone service		
425-214 Travel	3,000				3,000	211	2,789	7%	International Code Council Conferences		
425-218 Postage	1,500				1,500	68	1,432	5%	Certified Mailings		
425-220 Advertising/Legal Publications	500				500	-	500	0%	Job posting ads, public notices for nuisance properties, and property maintenance violation notices		
425-221 Training & Education	2,000				2,000	350	1,650	18%	International Code Council Conferences		
425-222 Dues & Subscriptions	500				500	5	495	1%	ICC Membership ($170), WV Code Official Dues ($40), Code Inspection License ($75), International Property Maintenance Code		
425-230 Contracted Services	25,000				25,000	-	25,000	0%			
425-230 Nuisance Properties - Contracted Services	68,000				68,000	-	68,000	0%	Nuisance Properties cleanup and demos. Supported by Rehab Funds.		
425-330 Nuisance Properties Relocation - Contracted Services	5,000				5,000	-	5,000	0%	Nuisance Properties housing relocation		
425-330 Vacant Properties - Contracted Services	24,000				24,000	500	23,500	2%	Allowance for vacant structures costs pertaining to Article 1759 Vacant Buildings. Supported by Vacant Structures Funds.		
425-341 Departmental Supplies	2,500				2,500	1,238	1,262	50%	Code books, door hangers, office supplies		
425-345 Uniforms	1,500				1,500	-	1,500	0%	Jackets & shirts		
TOTAL ENFORCEMENT AGENCY	**222,150**	**1,400**	**-**	**-**	**223,550**	**25,390**	**198,160**	11%			
REGIONAL DEVELOPMENT AUTHORITY - 435											
435-222 Dues & Subscriptions	11,500				11,500	11,304	196	98%	Region 9 Assessment		
TOTAL REGIONAL DEVELOPMENT AUTHORITY	**11,500**	**-**	**-**	**-**	**11,500**	**11,304**	**196**	98%			
TOTAL CITY ADMINISTRATION	**2,699,525**	**76,000**	**70,500**	**-**	**2,846,025**	**853,149**	**1,992,876**	30%			
BUILDING INSPECTIONS - 436											
436-103 Salaries	93,000				93,000	24,526	68,474	26%	Building Official/Inspector salary, 2.5% merit, holiday supplement, and clothing allowance		
436-104 FICA	7,500				7,500	1,871	5,629	25%	FICA @ 7.65% of Salary		
436-105 Group Insurance	1,310	790			2,100	671	1,428	32%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
436-106 Retirement	8,000				8,000	2,166	5,834	27%	PERS I & II Employer Contribution 8%		
436-109 OPEB	-				-	-	-		RHBT Insurance		
436-110 Fringe Benefits	3,000				3,000	722	2,278	24%	457(b) Deferred Compensation Employer Contribution (3%)		
436-211 Telephone	500				500	60	440	12%	Hot spot for tablet		
436-214 Travel	3,000				3,000	226	2,774	8%	ICC Conference; lodging, meals, gas		
436-220 Advertising/Legal Publications	500				500	-	500	0%	Job posting ads		
436-221 Training & Education	2,000				2,000	350	1,650	18%	ICC conferences and WV State Code Conference.		
436-222 Dues & Subscriptions	500				500	-	500	0%	ICC membership dues and Commercial & Residential Building inspection license		
436-223 Professional Services	50,000				50,000	3,875	46,125	8%	To cover expenses associated with inspections; compliance.		
436-341 Departmental Supplies	2,500				2,500	1,123	1,377	45%	Office supplies and code books		
436-345 Uniforms	1,500				1,500	-	1,500	0%	Jackets & shirts		
436-353 Computer Software/Tech	500				500	-	500	0%	Blue Beam-Plan review software		
TOTAL BUILDING INSPECTIONS	**173,810**	**790**	**-**	**-**	**174,600**	**35,590**	**139,010**	20%			

ACCOUNT	FY 2027 APPROVED BUDGET	REVISION #1	REVISION #2	REVISION #3	CURRENT BUDGET	FY 2027 YTD ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES AND EXPLANATIONS	REVISION #1 NOTES	REVISION #2 & #3 NOTES
PLANNING & ZONING - 437											
437-103 Salaries	361,000				361,000	84,041	276,959	23%	Assistant City Manager/Director of Community Development, Zoning Administrator, Permit Tech, and Long-Range Planner salaries, 2.5% merit, and holiday supplements		
437-104 FICA	29,000				29,000	6,330	22,670	22%	FICA @ 7.65% of Salary		
437-105 Group Insurance	54,000	19,000			73,000	13,927	59,073	19%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
437-106 Retirement	30,000				30,000	7,161	22,839	24%	PERS I & II Employer Contribution 8%		
437-108 Overtime	1,000				1,000	-	1,000	0%			
437-109 OPEB	750	1,700			2,450	502	1,949	20%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
437-110 Fringe Benefits	10,000				10,000	1,807	8,193	18%	457(b) Deferred Compensation Employer Contribution (3%)		
437-211 Telephone	1,000				1,000	126	874	13%	Director's department cell phone		
437-214 Travel	4,000				4,000	655	3,345	16%	James - American Planning Association Conference Alissa - WV Leadership Trainings (12 trainings) & Women Leaders in Code Wendy - MGO Conference		
437-218 Postage	1,000				1,000	-	1,000	0%	Certified mailings, legal notices, and yard sign postings		
437-220 Advertising/Legal Publications	4,500				4,500	323	4,177	7%	Advertising of BZA & public hearings for Planning Commission meetings; hearing placards; job posting ads		
437-221 Training & Education	5,000				5,000	-	5,000	0%	ICMA Gettysburg Leadership Institute ($1800), MGO Conference, Annual Conferences		
437-222 Dues & Subscriptions	3,500				3,500	286	3,214	8%	James AICP Membership ($550); Wendy ICC membership ($170); Alissa ICMA membership ($800) & WV Code Officials ($40); Adobe subscription ($1260).		
437-223 Professional Services	5,000				5,000	179	4,821	4%	GIS Aerial imagery, Background Checks		
437-230 Contracted Services	45,000				45,000	2,883	42,117	6%	Engineering and routine plan review; bond assessments		
437-238 Refunds	1,500				1,500	100	1,400	7%	Permit Refunds		
437-341 Departmental Supplies	3,250				3,250	456	2,794	14%	Public hearing signs, office supplies, and promotional supplies		
437-353 Computer Software / Tech	11,000				11,000	1,460	9,540	13%	MyPermit Now Monthly Fees (10,000), ArcGIS ($1000)		
TOTAL PLANNING & ZONING	**570,500**	**20,700**	-	-	**591,200**	**120,234**	**470,966**	20%			
TOTAL BUILD INSPECTION, P&Z, & ENFORCEMENT AGENCY	**$ 966,460**	**$ 22,890**	**$ -**	**$ -**	**$ 989,350**	**$ 181,214**	**$ 808,136**	18%			
ELECTIONS - 438											
438-220 Advertising/Legal Publications	500				500	-	500	0%	Publish ballot multiple times		
438-230 Contracted Services	5,000				5,000	-	5,000	0%	Poll workers compensation for early voting and day of election.		
438-341 Departmental Supplies	3,000				3,000	-	3,000	0%	Purchase of ballots $1,500, Election Kits, Paper, Election Banner, Voter Stickers		
TOTAL ELECTIONS	**8,500**	-	-	-	**8,500**	-	**8,500**	0%			
CITY HALL - 440											
440-103 Salaries	110,000			(20,000)	90,000	-	90,000	0%	Director of Operations Salary, 2.5% merit, and holiday supplement		Transfer to City Hall Bank Charges
440-104 FICA Taxes	8,800				8,800	-	8,800	0%	FICA @ 7.65%		
440-105 Group Insurance	22,000				22,000	-	22,000	0%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)		
440-106 Retirement	9,000				9,000	1	8,999	0%	PERS I & II Employer Contribution 8%		
440-109 OPEB	250	400			650	-	650	0%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
440-110 Fringe Benefits	3,700				3,700	-	3,700	0%	457(b) Deferred Compensation Employer Contribution (3%)		
440-211 Telephone	15,000				15,000	3,230	11,770	22%	WebEx Phone Services ($5,500), Cell phone - Director ($400), Rouss Hall Elevator & Fire Alarm Phone Service ($3,200), CWH Fire Alarm Phone Service ($2,000), City Hall Elevator & Fire Phone Service ($3000)		
440-213 Utilities	65,000				65,000	12,730	52,270	20%	City Hall Oil ($9000), City Hall Electric ($18,000), Rouss Hall Water & Electric ($4200), CW Hall Electric ($16,000), CW Hall Internet ($2000) & CH Internet ($12,000)		
440-214 Travel Expense	2,000				2,000	-	2,000	0%	WV Municipal League Election Training in Charleston, WV and annual HR conference		
440-215 Repair & Main. Bldg & Grounds	5,000				5,000	2,793	2,207	56%	City Hall, Rouss Hall, & CW Hall elevator services inspections and certifications.		
440-218 Postage	6,000				6,000	(577)	6,577	-10%	Pitney-Bowes Machine Postage; includes Treasurer's office mailings for B&O Tax Collection. Reflects increase in postage.		
440-219 Bldg & Equipment Rental	250,000				250,000	61,161	188,839	24%	CWH Loan ($200,000), CTUB Rent ($30,600), Postage Lease($1500), City Copier Rental, Plat Printer		
440-220 Advertising/Legal Publications	6,000				6,000	209	5,792	3%	American Legal Publishing online ordinance updates, job postings, and board vacancy advertisements		
440-221 Training & Education	1,000				1,000	-	1,000	0%	WV Municipal League Election Training in Charleston, WV and annual HR conference		
440-222 Dues & Subscriptions	6,500				6,500	530	5,970	8%	Jefferson County Chamber of Commerce ($275), WVML Annual Dues ($2,400), The Journal ($170), ICMA ($200), Amazon Prime ($130), Survey Monkey ($1650), Zoom ($1050)		
440-223 Professional Services	25,000				25,000	7,705	17,295	31%	Millenium Group insurance broker services estimated $1,800 per month, Open enrollment, payroll integration.		
440-226 Insurance & Bonds	220,000		20,000		240,000	232,252	7,748	97%	Liability, Worker's Comp, Auto Insurance, Umbrella, Commercial		Allowance for additional auto insurance for new vehicles and workers comp adjustment due to audit.
440-230 Contracted Services	235,000			(16,250)	218,750	39,566	179,184	18%	Sustainable Strategies (Grant Consultant, Matt Ward) - $60,000 ($5,000 per month) Website Hosting Fee (Revize) - $5700 per year for 5 years Pest Control Services - $1000 Patton Commercial Cleaning Services for City Hall and Rouss Hall - $15,000 Payroll Processing Base Fees - $12,000 Tek Advisors - $130,000 per year. Shredding Services - $500 Rouss Hall & CW Hall Alarm Services - $3500		Transfer to City Hall Other Fees/Taxes
440-232 Bank Charges	30,000			20,000	50,000	25,579	24,421	51%	Credit card merchant fees, eCheck Usage Fees, Fraud Detection Fees		Allowance for unexpected credit card processing fees
440-237 Other Fees/Taxes	1,500			16,250	17,750	16,257	1,493	92%	Ambulance fees		Allowance for Depot Distract property tax payment
440-341 Departmental Supplies	15,000				15,000	2,712	12,289	18%	City wide office supplies, toiletries, kitchen supplies, and water		
440-353 Computer Software / Tech	16,000		500		16,500	16,240	260	98%	Granicus Annual License - $10,000 - Agenda management, Online training, Audio/Visual software for livestreaming meetings VCS - $5000		Adjustment for increase in Granicus license.
TOTAL CITY HALL	**1,052,750**	**400**	**20,500**	-	**1,073,650**	**420,387**	**653,263**	39%			
CONTRIBUTIONS/TRANSFERS - 444											
444-568 Contributions - Community Partnership Grants	100,000				100,000	-	100,000	0%	Citizens Fire Co. $10,000; Independent Fire Co. $10,000; Library $20,000; Jef. Co. Com. Ministries $10,000; and EPTA $50,000.		
444-568 Community Grants		98,000			98,000	-	98,000	0%	Grant program for local non-profit organizations	Allowance for community grants for non-profit organizations	
444-568 Contributions - Annexation Support		103,000			103,000	-	103,000	0%		Contribution to support annexation costs	
444-568 Contributions - Revive Grant	30,000	229,000			259,000	25,000	234,000	10%	Revive! Program for small business commercial building upgrades in the downtown district.	$40,000 City Revive! grant funds awarded from FY 2026 and $189,000 remaining HUD grant from FY 2026	
444-568 Contributions - Façade Improvement Program	30,000	24,500			54,500	9,442	45,058	17%	Grant program to assist property owners and tenants in the Historic Overlay District to beautify property fronts	Grant funds awarded in FY 2026	
444-568 Contributions - Jefferson County P&R (Fireworks)	4,000				4,000	-	4,000	0%			
444-568 Contributions - Sidewalk Improvement Program	30,000	5,000			35,000	-	35,000	0%	Grant program to assist property owners with sidewalk repairs	Grant funds awarded in FY 2026	
TOTAL CONTRIBUTIONS/TRANSFERS	**194,000**	**459,500**	-	-	**653,500**	**34,442**	**619,058**	5%			

ACCOUNT	FY 2027 APPROVED BUDGET	REVISION #1	REVISION #2	REVISION #3	CURRENT BUDGET	FY 2027 YTD ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES AND EXPLANATIONS	REVISION #1 NOTES	REVISION #2 & #3 NOTES
PARKING - 571											
571-103 Salaries	49,000				49,000	11,555	37,445	24%	Parking Enforcement Officer salary, 2.5% merit, holiday supplement, and clothing allowance		
571-104 FICA Tax Expense	3,900				3,900	913	2,987	23%	FICA @ 7.65%		
571-105 Group Insurance	750	10,250			11,000	2,466	8,534	22%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
571-106 Retirement Expense	4,500				4,500	700	3,800	16%	PERS I & II Employer Contribution 8%		
571-108 Overtime	1,000				1,000	576	424	58%			
571-109 OPEB		650			650	151	499	23%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
571-110 Fringe Benefits	1,700				1,700	333	1,367	20%	457(b) Deferred Compensation Employer Contribution (3%)		
571-113 Utilities					-	-	-		Electric Service for parking lot - moved to Street Lights		
571-116 Repair & Main - Equipment	1,000				1,000	-	1,000	0%	Parking meter repairs and maintenance		
571-218 Postage	500				500	-	500	0%			
571-219 Bldg & Equipment Rental	500				500	-	500	0%			
571-220 Advertising / Legal Publications	500				500	-	500	0%	Job advertising		
571-230 Contracted Services	500				500	-	500	0%	Flu shot		
571-341 Departmental Supplies	5,000				5,000	4,363	637	87%	Office supplies, batteries, handheld printer paper		
571-345 Uniforms	750				750	470	280	63%	Jacket, shirts, patches, badge, etc.		
571-353 Computer Software/Tech	3,500		500		4,000	3,828	172	96%	United Public Safety/T2 annual fees		Allowance for UpSafety Hardware Care Program
TOTAL PARKING	**73,100**	**10,900**	**500**	**-**	**84,500**	**25,355**	**59,145**	30%			
TRANSFERS - 698											
698-590 Transfers to Capital Reserve - Repaving	150,000				150,000	48,958	101,042	33%	Monthly Street Fee Remittance from CTUB is transferred to Capital Reserve for future street repaving expenditures		
698-591 Transfers to Capital Reserve - One Time Funding		880,730			880,730	880,730	-	100%		Transfer to Capital Fund to support capital projects	
698-592 Transfers to Residual Fund		250,000			250,000	250,000	-	100%		Transfer to Residual Fund to build up Rainy Day savings	
698-591 Transfers to Capital Reserve - Table Games	950,000			100,407	1,050,407	63,436	986,971	6%	Transfer of race track lottery, limited video lottery, table games, and Greenbrier table games received in the general fund to the capital fund.		Transfer of insurance revenue to the Capital Fund for purchase of a new police car
TOTAL TRANSFERS	**1,100,000**	**1,130,730**	**-**	**100,407**	**2,331,137**	**1,243,123**	**1,088,014**	53%			
CONTINGENCIES - 699											
699-568 Other Contributions	450,000		(74,500)		375,500	-	375,500	0%	Placeholder for $50,000 for emergency snow costs. $250,000 for unexpected cost throughout the year. $150,000 for salary, FICA, and retirement increases based on salary study. (SAO caps this amount at 10% of receipts.)		
TOTAL CONTINGENCIES	**450,000**	**-**	**(74,500)**	**-**	**375,500**	**-**	**375,500**	0%			
POLICE DEPARTMENT - 700											
700-103 Salaries	1,765,000				1,765,000	424,367	1,340,633	24%	Base Salaries plus contingency, 2.5% merit, longevity, sign-on bonus, shift differential, clothing allowance, holiday supplement for (8) Patrolman/PFC, (4) Corporals, (3) Sergeants, (2) Lieutenants, (1) Captain, (1) Chief (3) Administrative personnel		
700-104 FICA	157,000				157,000	28,097	128,903	18%	FICA Tax at 7.65%		
700-105 Group Insurance	300,000	(35,000)			265,000	53,618	211,382	20%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Reduction in insurance costs due to changes in personnel	
700-106 Retirement	215,000				215,000	40,751	174,249	19%	Employer Retirement Contribution PERS I and II (9%) and MPFRS (8.5%)		
700-107 Police Pension	2,500				2,500	-	2,500	0%	Legacy CTPD Retirement System		
700-108 Overtime	200,000				200,000	62,996	137,004	31%	Shift coverage, late arrest/call out, special events, school events, court, etc.		
700-109 OPEB	5,000	6,000			11,000	2,257	8,743	21%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
700-110 Fringe Benefits	55,000				55,000	11,929	43,071	22%	457(b) Deferred Compensation Employer Contribution (3%)		
700-211 Telephone	12,000				12,000	2,413	9,587	20%	(4) department cell phones ($1750), WebEx phone services ($6300), Alarm phone line ($1350)		
700-213 Utilities	60,000				60,000	11,054	48,946	18%	Electric ($35,000), Internet Service ($12,000), MiFi/Cradle Points ($10,000)		
700-214 Travel	9,000				9,000	5,874	3,126	65%	Training, Conferences,etc. - (CALEA Conference 2nd Award - Omaha)		
700-215 R&M Building & Grounds	1,500				1,500	35	1,465	2%	Lights, Paint, Air Filters, Electrical supplies, Batteries		
700-216 R&M Equipment	10,000				10,000	-	10,000	0%	Generator service; radio & camera repair		
700-217 R&M Auto	50,000				50,000	29,803	20,197	60%	Air filters, vehicle repairs, state inspections, vehicle maintenance (brakes/rotors, tire repair/rotation, etc.)		
700-218 Postage	2,000				2,000	347	1,653	17%	Stamps, certified mail, UPS/FedEx, etc.		
700-219 Building & Equipment Rental	100,000				100,000	25,124	74,876	25%	661 Mortgage & copy machine leases		
700-220 Advertising/Legal Publications	5,500				5,500	1,588	3,912	29%	New Hire Ads 3-6 ads in local paper		
700-221 Training & Education	15,000				15,000	995	14,005	7%	WVSP Academy, 16 hours in-service/8 supervisor hours.		
700-222 Dues & Subscriptions	7,000				7,000	3,131	3,869	45%	WVCOP Dues, IACP, SRO, Journal, CALEA Annual Continuation Fee ($4,595)		
700-223 Professional Services	8,000	20,000			28,000	950	27,050	3%	Polygraph exams, psychological exam, physical exams, diagnostic imaging	Allowance for policy revision & CALEA Compliance	
700-223 Professional Services - Social Worker Services	75,000				75,000	75,000	-	100%	Third party social worker services		
700-230 Contracted Services	30,000				30,000	6,835	23,165	23%	Cleaning Fees ($12,000), HVAC Service Maintenance 661 George St. ($5500), Alarm service ($6400)		
700-237 Other Fees & Taxes	250				250	-	250	0%	661 George St. Ambulance Fees		
700-341 Departmental Supplies	35,000				35,000	5,280	29,720	15%	Ammunition, office Supplies, cleaning supplies, water delivery		
700-343 Auto Supplies (Gas, Oil & Tires)	70,000	30,000			100,000	28,341	71,659	28%	Gas, oil changes and tires for police vehicles	Allowance for increase in fuel prices	
700-345 Uniforms	35,000				35,000	8,076	26,924	23%	Class A, BDU, duty gear, insignia, ballistic vests ($4000 each), coats, etc.		
700-353 Computer Software/Tech	47,000				47,000	32,237	14,763	69%	Motorola - CAD ($12,200), Lexipole - Police One Academy ($1700), PowerDMS - Accreditation Documents ($4200), Motorola - In-Car & Body Camera Systems ($7000), RCN Technologies - Cradle Points Licensing ($3000), Target Solutions Guardian Tracking - ($1350), TLO - Investigative Research ($1320), All Traffic Solutions - Speed trailer software ($1500), Magnetic Forensics - cell phone download ($12,000)		
TOTAL POLICE DEPARTMENT	**3,271,750**	**21,000**	**-**	**-**	**3,292,750**	**861,097**	**2,431,653**	26%			
POLICE-SPECIAL DUTY CROSSING GUARDS - 704											
704-103 Salaries	40,000				40,000	4,665	35,335	12%	Five (5) Part-Time Crossing Guards (Wright Denny and Charles Town Middle). Expenses reimbursed by BOE. No COLA or merit. Holiday supplements.		
704-104 FICA Tax Expense	2,600				2,600	357	2,243	14%	FICA @ 7.65%		
704-341 Departmental Supplies	250				250	-	250	0%	Stop signs		
704-345 Uniforms	500				500	219	281	44%	Reflective jackets and vests		
TOTAL POLICE -SPECIAL DUTY CROSSING GUARDS	**43,350**	**-**	**-**	**-**	**43,350**	**5,240**	**38,110**	12%			
Total Police and Crossing Guards	**$ 3,315,100**	**$ 21,000**	**$ -**	**$ -**	**$ 3,336,100**	**$ 866,337**	**$ 2,469,763**	26%			

ACCOUNT	FY 2027 APPROVED BUDGET	REVISION #1	REVISION #2	REVISION #3	CURRENT BUDGET	FY 2027 YTD ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES AND EXPLANATIONS	REVISION #1 NOTES	REVISION #2 & #3 NOTES
DOG WARDEN - 707											
707-567 Contributions	1,800				1,800	-	1,800	0%	City donates the dog tag fees to the County Animal Control.		
TOTAL DOG WARDEN	**1,800**	-	-	-	**1,800**	-	**1,800**	0%			
MAINTENANCE - 750											
750-103 Salaries	327,057				327,057	76,069	250,988	23%	Director and (4) Maintenance Staff salaries, 2.5% merit, holiday supplements, clothing allowances and contingency for CDL, Playground Inspection, and ASE certifications.		
750-104 FICA Tax Expense	30,000				30,000	5,947	24,053	20%	FICA @ 7.65%		
750-105 Group Insurance	42,000	13,000			55,000	7,727	47,273	14%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
750-106 Retirement	28,000				28,000	6,884	21,116	25%	PERS I & II Employer Contribution 8%		
750-108 Overtime	20,000				20,000	2,262	17,738	11%			
750-109 OPEB	750	1,100			1,850	301	1,549	16%	RHBT Insurance	Allowance for anticipated retirement insurance increase	
750-110 Fringe Benefits	9,000				9,000	1,939	7,061	22%	457(b) Deferred Compensation Employer Contribution (3%)		
750-211 Telephone	2,000				2,000	222	1,778	11%	Field staff equipped with cell phones		
750-213 Utilities	10,000				10,000	836	9,164	8%	Maintenance building electric ($5000), water & sewer ($1500), and internet ($1200)		
750-214 Travel Expense	1,500				1,500	-	1,500	0%	Maintain certifications; other skill enhancement training as required/proposed		
750-215 R&M Buildings and Grounds	70,000	7,000			77,000	9,927	67,073	13%	General maintenance and repairs of all city buildings.	Allowance for HVAC repair at PD from FY 2026	
750-216 R&M Equipment	20,000				20,000	157	19,843	1%	Regular maintenance of fleet equipment, primary expense is street sweeper repairs.		
750-217 R&M Auto	10,000				10,000	3,655	6,345	37%	Regular maintenance of maintenance department and City vehicles		
750-219 R&M Bldg and Equip Rental	1,000				1,000	-	1,000	0%	Equipment rented as required to maintain various city buildings.		
750-220 Advertising	500				500	139	361	28%	Spring and Fall Cleanup. Additional city sponsored projects as required. Job advertising.		
750-221 Training & Education	5,000				5,000	-	5,000	0%	Maintain certifications; other skill enhancement training as required/proposed. CDL, Playground Inspection ($1000), ASE ($500), Certified Pool Operators ($2000), Arborist training ($1000).		
750-222 Dues & Subscriptions	500				500	-	500	0%	Camera subscription and CDL license fees		
750-223 Professional Services	500				500	45	455	9%	CDL physicals		
750-230 Contracted Services	50,000				50,000	7,501	42,499	15%	Trash service, box rental fees, snow removal and salt		
750-230 Contracted Services - Trees	20,000				20,000	-	20,000	0%	Tree services		
750-341 Departmental Supplies	40,000				40,000	5,904	34,096	15%	General maintenance supplies, Christmas decorations ($10,000), and light poles.		
750-343 Auto Supplies (Gas, Oil & Tires)	25,000	5,000			30,000	7,643	22,357	25%	Gas, oil changes and tires for maintenance department and City vehicles.	$4000 allowance for increase in fuel prices & $1000 allowance for Bobcat tires from FY 2026	
750-345 Uniforms	5,000				5,000	-	5,000	0%	Reflective jacket, shirts, vests, and pants		
TOTAL MAINTENANCE	**717,807**	**26,100**	-	-	**743,907**	**137,157**	**606,750**	18%			
STREET LIGHTS - 751											
751-213 Utilities	135,000				135,000	20,563	114,437	15%	Street lights electric (Increase for allowance of Stone Spring street lights)		
TOTAL STREET LIGHTS	**135,000**	-	-	-	**135,000**	**20,563**	**114,437**	15%			
P&R - 900											
900-103 Salaries	61,000				61,000	15,816	45,184	26%	Parks Manager salary, 2.5% merit, holiday supplement.		
900-104 FICA	5,000				5,000	1,195	3,805	24%	FICA @ 7.65%		
900-105 Group Insurance	10,000	1,000			11,000	2,557	8,443	23%	Health Insurance, Life Insurance, Dental Insurance, Vision Insurance. (Includes 3% premium increase projected by PEIA.)	Allowance for anticipated insurance costs	
900-106 Retirement	5,000				5,000	1,423	3,577	28%	PERS I & II Employer Contribution 8%		
900-109 OPEB	250	400			650	186	464	29%	RHBT Insurance	Allowance for anticipated retirement insurance increase.	
900-110 Fringe Benefits	2,000				2,000	339	1,661	17%	457(b) Deferred Compensation Employer Contribution (3%)		
900-211 Telephone	600				600	95	505	16%			
900-214 Travel Expense			2,000		2,000	615	1,385	31%			Lodging, gas, meals, airfare for training conferences.
900-221 Training & Education			1,500		1,500	-	1,500	0%			NRPA National Conference
900-341 Departmental Supplies	750				750	-	750	0%	Office supplies		
900-566 Contributions	107,500				107,500	34,383	73,117	32%	50% Hotel/Motel tax revenue to support Pool/Tennis/Park expenses in the Parks & Rec budget. Additional $20,000 donation from the City to the P&R for these expenses.		
TOTAL P&R	**$ 192,100**	**$ 1,400**	**$ 3,500**	**$ -**	**$ 197,000**	**$ 56,611**	**$ 140,389**	29%			
VISITOR'S CENTER - 901											
901-567 Contributions	87,500				87,500	14,383	73,117	16%	50% of Hotel/Motel Tax Revenue Contribution to Jefferson County Visitor's Center.		
TOTAL VISITOR'S CENTER	**87,500**	-	-	-	**87,500**	**14,383**	**73,117**	16%			
FAIRS/FESTIVALS - 903											
903-220 Advertising/Legal Publications	2,000				2,000	-	2,000	0%	Event Advertising		
903-230 Contracted Services	35,000				35,000	4,646	30,354	13%	Stage/Sound ($5,000), Musicians ($5,000), Athlete Appearances ($10,000), Signage ($2,000), Inflatables ($2,000), Portable toilets ($1,000), Hospitality/lodging and meals for talent ($2,000), Shuttle bus ($1,500), Game Entertainment Avenue ($2,000) and other miscellaneous entertainment. **Car Show** Sound ($2,500), Announcer ($500), Model T Ford Car Club ($600), Porta Potts ($900), Gaming Trailer ($1,000)		
903-238 Refunds	100				100	-	100	0%			
903-341 Departmental Supplies	25,000				25,000	5,137	19,863	21%	**WV Fest** Water/cups ($1,500), Tents ($1,500), Art Supplies ($800), Chairs & Railing ($1,000), Signage ($1,500) **Car Show** Trophies/Plaques ($4,700), Signage/Parking ($500), Water/Chips ($1,500) **General** Candy ($2,000), Contest prizes for Light the City and Xmas parade ($1,625), Christmas costumes, Signs ($500)		
903-568 Contributions	5,000				5,000	2,500	2,500	50%	Donations to the Boys & Girls Club, High School Choir, and Jefferson High School Air Force ROTC.		
TOTAL FAIRS/FESTIVALS	**67,100**	-	-	-	**67,100**	**12,283**	**54,817**	18%			
TOTAL EXPENSES	**9,785,842**	**1,747,120**	-	**100,407**	**11,633,368**	**3,419,226**	**8,214,142**	29%			
REVENUES OVER EXPENSES	$ 0	$ (0)	$ -	$ -	$ (0)	$ 2,298,188					

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2049: FY2027 Capital Fund Budget Revision #2

ATTACHMENTS:

- FY 2027 Capital Budget 2nd Revision.pdf

the city of Charles Town, WV

FY 2027 Capital Reserve Budget

ACCOUNT	FY 2027 BUDGET	REVISION #1 PROPOSAL	REVISION 2 PROPOSAL	FY 2027 CURRENT BUDGET	FY 2027 YEAR TO DATE ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES	REVISION #1 NOTES	REVISION #2 NOTES
CAPITAL BUDGET REVENUES										
Capital Reserve Carryover	4,130,854	2,398,696		6,529,550	$ 6,529,550	$ (0)	100%	$2,063,655 carryover balance from FY2026 Capital Reserve. This is carryover for unfinished projects noted in red. $2,067,199 additional grant carryover transferred to the grant projects worksheet. (Carryover will be adjusted in the 1st Revision in July 2026.)	Adjust carry over amount to actual balance as of June 30, 2026	
368-000 Contributions from GF		880,730		880,730	$ 880,730	$ -	100%	Contributions from GF (Determined in July 2026 1st Revision)		
368-000 Contributions from GF - Lottery / Gaming Revenue	950,000		100,407	1,050,407	$ 63,436	$ 986,972	6%	All lottery/gaming revenue remitted to Charles Town gets transferred to Capital Reserve from General Fund.		Insurance proceeds contributed from the GF for purchase of a replacement police vehicle
341-000 Developer Proffers	255,000			255,000	$ 104,420	$ 150,580	41%	Developer Proffer fees.		
380-000 Interest on Bank Accounts & Other Sources	100,000			100,000	$ 15,121	$ 84,879	15%			
TOTAL REVENUES	**$ 5,435,854**	**$ 3,279,426**	**$ 100,407**	**$ 8,815,687**	**$ 7,593,257**	**$ 1,222,430**	**86%**			

ACCOUNT	FY 2027 BUDGET	REVISION #1 PROPOSAL	REVISION 2 PROPOSAL	FY 2027 CURRENT BUDGET	FY 2027 YEAR TO DATE ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES	REVISION #1 NOTES	REVISION #2 NOTES
CAPITAL BUDGET EXPENSES										
975 GENERAL GOVERNMENT										
Information Technology										
Computer Replacement - 975-459 General Government Capital Outlay Technology	25,000			25,000	$ -	$ 25,000	0%	Computer replacement program for all General Government departments. (5 replacements are planned.)		
Tyler Tech Version 10 Software - 975-459 General Government Capital Outlay Technology	55,130			55,130	$ 250	$ 54,880	0%	Centralized Finance/Permitting/Zoning/Grants/Bond Tracking Software. This software will replace GoGov, MyGov, PSI, and enhance Incode. Having a centralized software will improve efficiency and reduce duplication of work. This software takes a year to implement. ($55,130 carried over from FY26.)		
TOTAL INFORMATION TECHNOLOGY	**$ 80,130**	**$ -**	**$ -**	**$ 80,130**	**$ 250**	**$ 79,880**	**0%**			
Other - General Government										
City Charter Re-write - 975-223 General Government Professional Services		60,000		60,000	$ -	$ 60,000	0%			
Comprehensive Plan Update - 975-223 General Government Professional Services		125,000		125,000	$ -	$ 125,000	0%		Professional services to update the City's policy guide for decision making pertaining to future land use, growth & development, & resource preservation within the City's jurisdiction and Urban Growth Boundary	
Finance Police Re-write - 975-223 General Government Professional Services			50,000	50,000	$ -	$ 50,000	0%			Allowance for the comprehensive review and revision of the City's financial policies.
Rouss Hall Landlord buy back - 975-458 General Government Capital Outlay	140,000			140,000	$ -	$ 140,000	0%	$140,000 carried over from FY26.		
Zoning & Subdivision Ordinance Overhaul - 975-223 General Government Professional Services	172,850			172,850	$ -	$ 172,850	0%	Outsourcing costs to update this ordinance. It has not been updated since 2012 - This is a 2 year plan for a total of $250,000. ($172,850 carried over from FY26.)		
Front Office Desks - 975-459 General Government Equipment	3,300			3,300	$ 3,205	$ 95	97%	$3300 carried over from FY26.		
TOTAL OTHER - GENERAL GOVERNMENT	**$ 316,150**	**$ 185,000**	**$ 50,000**	**$ 551,150**	**$ 3,205**	**$ 312,945**	**1%**			
TOTAL GENERAL GOVERNMENT	**$ 396,280**	**$ 185,000**	**$ 50,000**	**$ 631,280**	**$ 3,455**	**$ 392,825**	**1%**			

ACCOUNT	FY 2027 BUDGET	REVISION #1 PROPOSAL	REVISION 2 PROPOSAL	FY 2027 CURRENT BUDGET	FY 2027 YEAR TO DATE ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES	REVISION #1 NOTES	REVISION #2 NOTES
976 PUBLIC SAFETY										
Equipment										
Body Worn Cameras - 976-460 Public Safety Capital Outlay Equipment		32,000		32,000	$ -	$ 32,000	0%		Replace 19 body worn cameras with expired warranties. Version V700	
Office Chairs - 976-460 Public Safety Capital Outlay Equipment		8,100		8,100	$ -	$ 8,100	0%		Replace 24 dilapidated office chairs.	
Officer Equipment - 976-460 Public Safety Capital Outlay Equipment	17,500			17,500	$ 7,175	$ 10,325	41%	Equipment for new officer. (Taser, ballistic shield, baton, spike system, trauma aid kit, trauma pac kit, defibrillator, body worn camera, and desktop computer)		
TOTAL EQUIPMENT	**$ 17,500**	**$ 40,100**	**$ -**	**$ 57,600**	**$ 7,175**	**$ 10,325**	**12%**			
Information Technology										
Computer Replacement - 975-460 General Government Capital Outlay Technology Police Department	33,000			33,000	$ -	$ 33,000	0%	6 In-car Panasonic Tough Tablets (To replace generation 3 reaching end of life.)		
TOTAL INFORMATION TECHNOLOGY	**$ 33,000**	**$ -**	**$ -**	**$ 33,000**	**$ -**	**$ 33,000**	**0%**			
Vehicles										
Police Cars - 976-459 Public Safety Capital Outlay Vehicles	144,000			144,000	$ 140,850	$ 3,150	98%	PD requests 2 vehicles per rotation schedule based on vehicle lifespan of 7 years. A third vehicle is requested this year for the new officer position.		
Police Vehicle Upfit Costs - 976-459 Public Safety Capital Outlay Vehicles	48,000			48,000	$ 24,286	$ 23,714	51%	Approximately $5000 per car is estimated for the 2 vehicles in the rotation schedule. This amount is for equipment installation labor. Equipment was purchased in FY25 through the COPS Grant. Cost for 3rd car is $38,000.		
Replacement Police Vehicle & Upfit Costs - 976-459 Public Safety Capital Outlay Vehicles			100,407	100,407	$ -	$ 100,407	0%			Allowance for purchase of a replacement police cruiser and corresponding upfitting costs
TOTAL VEHICLES	**$ 192,000**	**$ -**	**$ 100,407**	**$ 292,407**	**$ 165,136**	**$ 127,271**	**56%**			
Parking										
Parking Meters - 976-462 Public Safety	5,000			5,000	$ 4,824	$ 176	96%	23 Parking meter mechanisms the replace the outdated Duncan meters as part of the replacement system implemented over the last 2 years.		
TOTAL PARKING	**$ 5,000**	**$ -**	**$ -**	**$ 5,000**	**$ 4,824**	**$ 176**	**96%**			
TOTAL PUBLIC SAFETY	**$ 247,500**	**$ 40,100**	**$ 100,407**	**$ 388,007**	**$ 177,135**	**$ 170,772**	**46%**			

ACCOUNT	FY 2027 BUDGET	REVISION #1 PROPOSAL	REVISION 2 PROPOSAL	FY 2027 CURRENT BUDGET	FY 2027 YEAR TO DATE ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES	REVISION #1 NOTES	REVISION #2 NOTES
977 STREETS & TRANSPORTATION										
Buildings										
Charles Washington Hall - Roof Replacement - 977-457 Streets & Transportation Capital Outlay Buildings	50,000			50,000	$ 6,767	$ 43,233	14%	This is a small section of the rooftop that contains 4 rooftop AC units. This area has failed sealant and degraded membranes. It will be replaced with a 2 Ply-Cold System which has a useful life of 30 years. ($50,000 carried over from FY26.)		
Charles Washington Hall - Painting of Exterior Windows/Doors/Trim - 977-457 Streets & Transportation Capital Outlay Buildings		60,000		60,000	$ -	$ 60,000	0%		Painting of all outside wood surfaces at CWH. (Windows, doors, soffit, and facia)	
City Hall - Brick Repointing - 977-457 Streets & Transportation Capital Outlay Buildings		40,000		40,000	-	$ 40,000	0%		Repair damaged mortar at City Hall.	
City Hall - Elevator Replacement - 977-457 Streets & Transportation Capital Outlay Buildings		70,000		70,000	-	$ 70,000	0%		Replace City Hall elevator car and mechanical units.	
City Hall - Replace Rooftop AC Units - 977-457 Streets & Transportation Capital Outlay Buildings	45,730			45,730	$ -	$ 45,730	0%	Replacement of 2 City Hall rooftop AC units. ($45,730 carried over from FY26.)		
City Hall - Restore Roof Section 2 - 977-457 Streets & Transportation Capital Outlay Buildings		20,000		20,000	$ -	$ 20,000	0%		Section 2 of the City Hall roof is in poor condition. This is an allowance to restore that area of the roof.	
Maintenance Yard Study & Engineering - 977-457 Streets & Transportation Capital Outlay Buildings	220,700			220,700	$ -	$ 220,700	0%	Maintenance yard study. Current maintenance yard is in poor condition and needs replaced or renovated. In FY26 Council requested that a study be conducted for the best location of the Maintenance Yard along with associated engineering. The engineering remains to be completed. ($220,700 carried over from FY26.)		
Rouss Hall - Brick Repointing -977-457 Streets & Transportation Capital Outlay Buildings		20,000		20,000	$ -	$ 20,000	0%		The west wall is severely deteriorated. This will provide an allowance to repair the mortar.	
Rouss Hall - Paint Exterior/Repair Rotted Sills - 977-457 Streets & Transportation Capital Outlay Buildings	209,975			209,975	$ -	$ 209,975	0%	All window sills at Rouss Hall have peeling paint and rotted wood. ($209,975 carried over from FY26.)		
Rouss Hall - Apply roof coating - 977-457 Streets & Transportation Capital Outlay Buildings	31,250			31,250	$ -	$ 31,250	0%	The roof is rusting and has degraded metal panels. It will be replaced with a Cool Sil System which has a useful life of 10 years. ($31,250 carried over from FY26.)		
TOTAL BUILDINGS	**$ 557,655**	**$ 210,000**	**$ -**	**$ 767,655**	**$ 6,767**	**$ 760,888**	**1%**			

ACCOUNT	FY 2027 BUDGET	REVISION #1 PROPOSAL	REVISION 2 PROPOSAL	FY 2027 CURRENT BUDGET	FY 2027 YEAR TO DATE ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES	REVISION #1 NOTES	REVISION #2 NOTES
Streets/Infrastructure										
Art Alley Brick Stamped Pavement - 977-458 Streets & Transportation Capital Outlay Other Improvements		25,000		25,000	$ -	$ 25,000	0%		Repave Art Alley and apply brick imprint.	
Brick Sidewalk Replacement - Washington St. - 977-458 Streets & Transportation Capital Outlay Other Improvements		55,000		55,000	$ -	$ 55,000	0%		Replace brick sidewalk from the Post Office on W. Washington Street to 120 S. George St.	
Charles Street Engineering Study - 977-461 Streets & Transportation Capital Outlay Stormwater Improvements	79,975	290,000		369,975	$ -	$ 369,975	0%	Concept Plan for the shared street and event space shovel ready design for Charles Street. This document will assist with grant applications. ($79,975 carried over from FY26.)	Allowance to produce engineering-ready documents to make storm water corrections, bury utility lines, level the street, and transform streetscape into usable event space.	
Depot Square Design - 977-458 Streets & Transportation Capital Outlay Other Improvements	50,000		(50,000)	-	$ -	$ -		Design for potential uses and amenities of the City's new town square. ($50,000 carried over from FY26.)		Transfer to Parks Master Plan
Sidewalks (ADA) & stormwater drain for Lawrence/Congress - 977-458 Streets & Transportation Capital Outlay Other Improvements	100,000			100,000	$ -	$ 100,000	0%	Stormwater repair and ADA sidewalks for the Lawrence & Congress intersection. Grant match was paid in FY26. This is an allowance for overages. Reduction Funding. ($5240 carried over from FY26.)		
Stormwater Assessment Study - 977-461 Streets & Transportation Capital Outlay Stormwater Improvements	125,955	228,825		354,780	$ -	$ 354,780	0%	This funding is a 2 year plan to cover 6 study areas and 3 area reviews each year. ($125,955 carried over from FY26.)	Allowance to proceed to the full inventory and detailed analysis of Watersheds 1, 2, 3, 7, & 10	
TOTAL STREETS/INFRASTRUCTURE	**$ 355,930**	**$ 598,825**	**$ (50,000)**	**$ 904,755**	**$ -**	**$ 824,755**	**0%**			
Vehicles										
Bucket Truck - 977-459 Streets & Transportation Capital Outlay Equipment	175,000			175,000	$ 166,890	$ 8,110	95%	Current bucket truck cannot safely reach the required heights for maintenance tasks. The cost of a new truck is approximately $170,000. The truck will be ordered in FY25 and received in July of FY27. ($175,000 carried over from FY26.)		
Dump Truck - 977-459 Streets & Transportation Capital Outlay Equipment		90,000		90,000	$ -	$ 90,000	0%		This dump truck includes a landscaping dump bed for hauling brush and snow	
Street Sweeper - 977-459 Streets & Transportation Capital Outlay Equipment	350,000			350,000	$ 344,890	$ 5,110	99%	The current sweeper is unreliable and constantly being repaired.		
Pick-up Truck - 977-459 Streets & Transportation Capital Outlay Equipment	$ 70,000			70,000	$ -	$ 70,000	0%	Replacement of 2016 truck to include emergency lighting and utility bed.		
TOTAL VEHICLES	**$ 595,000**	**$ 90,000**	**$ -**	**$ 685,000**	**$ 511,780**	**$ 173,220**	**75%**			
Streets & Transportation Other										
Charles Washington Hall - 2 Refrigerators - 977-459 Streets & Transportation Capital Outlay Equipment		8,000		8,000	$ 6,435	$ 1,565	80%		2 commercial refrigerators on 1st floor of Charles Washington Hall. (8000 carried over from FY26)	
Maintenance Yard Storage Containers - 977-459 Streets & Transportation Capital Outlay Equipment		25,000		25,000	$ -	$ 25,000	0%			
Trash Can Replacement - Downtown - 977-459 Streets & Transportation Capital Outlay Equipment		70,000		70,000	$ -	$ 70,000	0%		Replace 40 deteriorating trash in the Downtown District	
TOTAL STREETS & TRANSPORTATION OTHER	**$ -**	**$ 103,000**	**$ -**	**$ 103,000**	**$ 6,435**	**$ 96,565**	**6%**			
TOTAL STREETS & TRANSPORTATION	**$ 1,508,585**	**$ 1,001,825**	**$ (50,000)**	**$ 2,460,410**	**$ 524,982**	**$ 1,855,428**	**21%**			

ACCOUNT	FY 2027 BUDGET	REVISION #1 PROPOSAL	REVISION 2 PROPOSAL	FY 2027 CURRENT BUDGET	FY 2027 YEAR TO DATE ACTUAL	FY 2027 BUDGET BALANCE	% OVER/UNDER BUDGET	NOTES	REVISION #1 NOTES	REVISION #2 NOTES
979 CULTURE & RECREATION										
Parks & Recreation										
Jefferson Memorial Park Tennis Court Resurfacing & Fencing - 979-458 Culture & Recreation Other Improvements		300,000		300,000	$ -	$ 300,000	0%		Mill, pave, and apply acrylic sport court coating on the tennis courts. Install chain link fencing around the courts.	
Parks Master Plan - 979-223 Culture & Recreation Professional Services	150,000		50,000	200,000	$ -	$ 200,000	0%			Funds to combine Depot District Design planning with Parks Master Plan
TOTAL PARKS & RECREATION	**$ 150,000**	**$ 300,000**	**$ 50,000**	**$ 500,000**	**$ -**	**$ 200,000**	**0%**			
Culture										
Christmas lights replacement along Washington & George Streets - 979-458 Culture & Recreation Other Improvements	25,000			25,000	$ 12,256	$ 12,744	49%	Current lights are failing and need to be replaced.		
Historical Signs - 979-458 Culture & Recreation Other Improvements	10,000			10,000	$ -	$ 10,000	0%			
Wayfinding signage - 979-458 Culture & Recreation Other Improvements	297,400			297,400	$ -	$ 297,400	0%	CDD REQUEST $100K for Wayfinding Signage implementation (3 years of phases at $100,000 per year ending in FY27.) (Request related to 2023 CTNOW ARPA Request) ($197,400 carried over from FY26.)		
TOTAL CULTURE	**$ 332,400**	**$ -**	**$ -**	**$ 332,400**	**$ 12,256**	**$ 320,144**	**4%**			
TOTAL CULTURE AND RECREATION	**$ 482,400**	**$ 300,000**	**$ 50,000**	**$ 832,400**	**$ 12,256**	**$ 520,144**	**1%**			
Building Improvements Contingency	349,160			349,160	$ -	$ 349,160	0%	Developer fees transferred from Building Commission in FY 2026 to the Capital Fund. This is the remaining balance as of 6/30/26. ($349,160 carried over from FY26.)		
Contingencies	384,730	1,752,501	(50,000)	2,087,231	$ -	$ 2,087,231	0%	This amount will be adjusted in the 1st Revision in July 2026.		Transfer of funds to Finance Policy Re-write
Encumbrances for Subsequent Years				-	$ -	$ -				
Transfer to Grant Projects	2,067,199			2,067,199	$ -	$ 2,067,199	**0%**	$76,444 to Augustine Avenue Project. $1,990,755 to JMP Pool Project.		
TOTAL EXPENSES	**$ 5,435,854**	**$ 3,279,426**	**$ 100,407**	**$ 8,815,687**	**$ 717,829**	**$ 7,442,758**	**8%**			
REVENUES OVER EXPENSES	**$ -**	**$ (0)**	**$ -**	**$ (0)**	**$ 6,875,428**					

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2050: Vacant Structure Building Registry Appeal - Vacant Structures Code Exemption Procedures Policy

ATTACHMENTS:

- Vacant Structure Code Exemption Procedures Final.pdf

Vacant Structures Code Exemption Procedures

1. **Scope and Application**. This regulation governs the process to apply for exemption from the requirement to register a structure as vacant under the City of Charles Town ("City") Vacant Structures Code, codified at Article 1759 of the City Code, as it may be amended, supplemented, or replaced. The terms used in this regulation shall have the same meanings as those given in Article 1759 of the City Code unless another definition is specifically supplied by this regulation.

2. **Purpose**. Exemption from registration under the Vacant Structures Code is authorized by City Code Section 1759.06(a) and required as part of any local vacant structures code by W. Va. Code § 8-12-16c(b)(2), which provides that "The governing body of a municipality, on a case-by-case basis, upon request by the property owner, shall exempt a vacant building from registration upon a finding for good cause shown that the person will be unable to occupy the building for a determinant (*sic*)[1] period of time."

3. **Application for Exemption**. The owner of a "vacant building," as defined by City Code 1759.02(j) may request exemption from the registration requirements of Article 1759 by filing in the form prescribed by the City. The request shall be submitted to the City Clerk either by personal delivery or e-mail to the City Clerk's office during the City business hours or by mail to "The City of Charles Town, c/o City Clerk, 101 E. Washington Street, Charles Town, WV 25414.

4. **Determination of Completeness**. The City Manager or designee will review all submitted applications to determine if they contain enough information to be considered by City Council. Only applications that contain information outlining the grounds for an exemption will be forwarded to City Council for consideration.

5. **Delivery to City Council**. Upon a determination that the application is complete, the City Manager, or a designee, will submit the application to City Council and place the application for hearing on an agenda for a regular meeting for which notice of the request can be adequately provided in accordance with the law, or at a special meeting called for the purpose of hearing the application. The City Manager, or a designee, will inform the applicant by email of the date and time of the hearing and may provide the Applicant with a copy of Section 1759 of the City Code, if a copy has not previously been provided.

6. **Documentation or Recommendation submitted to City Council**. The applicant may submit any documentation in support of the application, which is not already contained in the application, no later than noon one business day prior to the hearing before City Council. The City Manager, or a designee, may, but shall not be required to, submit any recommendation on the application and any supporting material no later than noon one business day prior to the hearing before City Council. When submitting material to City Council, the applicant shall deliver the material to the City Manager by email on the same day. When submitting material to City Council, the City Manager or designee shall deliver the material to the applicant by email on the same day. These requirements for submission of documentation apply to all forms of media including written and electronic materials in any form. If any participant in the hearing wishes to present material by electronic means, such as powerpoint or video presentation, the submission of documentation shall include a written request to City Council to permit the electronic

presentation.

7. **Hearing by City Council**. On the date and time set for the hearing, the hearing will proceed as follows:

    a. **Electronic media**. Prior to hearing any presentation, City Council will determine whether to permit presentations using electronic media, if a request has been submitted in accordance with this regulation. City Council may elect to permit or decline the use of electronic media in its sole discretion.

    b. **City Manager recommendation**. Following a determination on the use of electronic media, if needed, City Council will allow the City Manager or a designee to present a recommendation, if any, on the application. The City Manager shall have five (5) minutes to present the recommendation, and Council may extend the time in its discretion upon request.

    c. **Applicant recommendation**. Following the presentation of the City Manager, if any, the applicant or a designee may make a presentation in support of the exemption application. The applicant may make the presentation directly or by third parties – including legal counsel – or by a combination of those methods. The applicant shall have five (5) minutes to make the presentation, and Council may extend the time in its discretion upon request

    d. **Witness testimony**. City Council will not swear witnesses or take witness testimony during the hearing.

    e. **Questioning by City Council**. Following the conclusion of the presentations, City Council may ask questions of any person participating in the presentations.

    f. **Standard of Review**. City Council will determine whether an applicant has demonstrated (i) good cause, (ii) that the applicant will be unable to occupy the building, (iii) for a certain period of time. For purposes of these rules, good cause supporting the inability to occupy a building means a legal or practical issue that is outside the control of the property owner and which would prevent occupancy of the building despite reasonably diligent efforts by the property owner to occupy the building or permit occupancy by another person. Such good cause may include, subject to the discretion of City Council in each individual case, the existence of contested claims to ownership of the property that cannot be resolved by the property owner and do not allow occupancy of the building, including claims made in probate or other testamentary transfer proceedings; the ongoing renovation of a building necessary to make it fit for occupancy and compliant with law, so long as such renovation is diligently pursued; or the ongoing attempt to sell the building to a new owner, so long as the property is continuously listed for sale, the property owner is actively participating in marketing the property for sale, the property owner is willing to accept purchase offers reasonably approximating the market value of the property, and other occupancy of the property during the marketing period is either not permitted by law or would substantially interfere with the sale of the property. Good cause for exemption does not include disrepair of the property or violations of law at the property, unless the applicant has demonstrated an ongoing renovation

identified in the preceding sentence; difficulties in sale or occupancy of the property due to market conditions when an occupant might reasonably be found at current market prices or rates; nor the property owner's absence from the property, even with intent to return, absent additional factors as may be described in the preceding sentence. If the applicant has not established all three elements supporting the exemption to the satisfaction of Council, the application for exemption will be denied. If the applicant has established all three elements supporting the exemption to the satisfaction of Council, the application for exemption will be granted.

g. **Decision on Application**. Upon the conclusion of questioning by City Council, if any, the Council may (i) make a decision on the application, (ii) take the matter under advisement for future decision, or (iii) request or allow the participants to submit any additional information that may assist in the decision, including proposed findings and conclusions on the application. The decision by City Council shall be reduced to writing and delivered to the applicant by email. Any decision granting exemption must specify a certain date upon which the exemption expires. The period for which an exemption is granted shall not extend beyond the next annual registration date required by *City Code* § 1759.03. Applicants may seek additional exemptions for a property, when the exemption period has expired or will expire, by submitting a new application in accordance with this regulation.

h. **Application of Open Governmental Proceedings Act**. When acting on an application for exemption from the Vacant Structures Code registration requirements, City Council is making an adjudicatory decision in a quasi-judicial or administrative capacity. Accordingly, the proceedings do not constitute a "meeting" within the definition provided by the Open Governmental Proceedings Act. *See W. Va. Code* § 6-9A-2(5)(A). City Council may choose to conduct all or any part of the proceedings in closed session.

i. **Effect on application of Vacant Structures Code**. The pendency of an application for exemption does not abrogate the duty of the property owner to comply with the Vacant Structures Code, including any requirement to pay registration fees. A decision by City Council to grant exemption may include a determination to waive or refund registration fees due or paid. An exemption granted by City Council may be used as a defense by the property owner in any pending criminal action for failure to register the vacant building subject of the exemption.

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2052: Greenway Engineering Study - Watershed 3 Next Steps

The Infrastructure Committee recommends moving forward with all needed next phases to bring shovel ready solutions to Watershed 3 (from the Greenway Engineering study).

ATTACHMENTS:

- 7037.07P2 CCT Watershed 3 Pt 2-3 Proposal 101326 - GE Signed.pdf
- Watershed 3 Greenway Stormwater.pdf

GREENWAY ENGINEERING
704 Foxcroft Avenue
Martinsburg, WV 25401

October 13, 2026

Steve Galleher, Operations Director
City of Charles Town
101 E. Washington Street
Charles Town, WV 25414

Re: **City of Charles Town – Downtown Stormwater Study**
Drainage Shed 3, Part 2 and 3 – Full Analysis and Inventory, Improvement Analysis
Engineering and Surveying Services Proposal

Dear Mr. Galleher:

Greenway Engineering, Inc. (Greenway) is pleased to offer this proposal to The City of Charles Town (Client) in effort to provide engineering services for Part 2 of the Downtown Stormwater Study (Project) in the City of Charles Town, West Virginia. The project consists of the City of Charles Town's Watershed #3 which consists of approximately 30 acres and primarily encompasses the following streets: Shutter, Wall, Beckwith and the George Street Extension. Our scope of services is as follows:

Part 2 – Full Analysis and Inventory - Watershed 3

Item 3.2A Full Inventory

Greenway will complete a full field as-built survey of the storm water infrastructure identified in Part 1 of the study for the watershed. The storm sewer associated with the CTUB WWT facility along George Street will be excluded from detailed survey and analysis as the system has no identified issues and is wholly contained within the parcel owned by CTUB. Greenway will coordinate with City maintenance staff to facilitate full access to structures that are not readily accessible by field crews. If the scope of work to gain access to structures/conduits is above capabilities of the City maintenance department, the City will be responsible for contractor procurement and cost. Greenway will help coordinate scope of work and schedule for contractors as needed under **Item 3.A** listed below. As part of the full inventory process, Greenway will note any indicators of sanitary sewer tied to the storm sewer and provide the information to the City, however it will not include a full study of sanitary/storm cross connections. Camera work and/or siltation removal may be required for areas of the storm sewer not accessible or that present significant concern for debris/siltation within the storm sewer pipes. The fee provided is not inclusive of camera and/or siltation removal.

FEE: $8,500
Lump Sum
Item 3.2A

Item 3.2B Final Hydrological and Hydraulic Analyses

Final analysis of the inventoried system will be performed including inlet capacity checks, hydraulic grade line modeling, and flow/volume approximation. The analysis will also be performed for future conditions based on the comprehensive plan. The analyses will utilize SCS TR-55, SCS TR-20, and

Rational analyses as determined relevant or appropriate. The 500yr, 100yr, 10yr, 2yr, and 1" water quality flows and volumes will be analyzed.

FEE: $12,980
Lump Sum
Item 3.2B

Item 3.2C Priority List

Greenway will refine the list of all capacity/flooding concerns within the watershed. Greenway will confer with the city on issues identified and assist with prioritizing each capacity/flooding concern by providing input on the severity of each identified issue based on the final analysis completed with **Item 3.2B**. If the City desires public outreach and input to be incorporated in the prioritization of the list Greenway can assist as requested under **Item 3.A**. The scope of this task includes 2 meetings with city officials and time to refine a formatted priority list with descriptions of the issues and their suspected impacts.

FEE: $4,700
Lump Sum
Item 3.2C

Deliverables for Part 2

1. Detailed map of Watershed 3 and associated stormwater infrastructure and conveyance systems. This will be incorporated into the documentation provided during Part 1.
2. Plan and profile views of existing infrastructure, conveyance systems including modeled hydraulic grade lines, and water surface elevations as appropriate within Watershed 3.
3. List of potential capacity and flooding concerns prioritized through coordination with the City.
4. Updated ESRI GIS Shapefiles of watershed 3 outlines and locations of identified drainage infrastructure/ conveyance systems.

Part 3 – Improvement Analysis - Watershed 3

Item 3.3A Concept Development

Greenway will develop 2 conceptual solutions for the Watershed 3 drainage issues. The first concept will outline a comprehensive solution that will address all issues identified within the watershed in the Part 1 report. The second concept will address the highest priority issues while seeking to minimize needed easements and construction costs. The concepts will be reviewed with City officials, and Greenway will provide technical input to assist the city with concept selection. This will include outlining the potential easements needed, if any, so that easement acquisition can be included in feasibility discussions. Should additional concepts be desired they will be processed under the additional fee noted below.

FEE: $7,250, Lump Sum
FEE: $2,975, Each Additional Concept, Lump Sum
Item 3.3A

Item 3.3B Schematic Design

Greenway will develop a schematic design based on the selected concept from **Item 3.3A**. The schematic will depict expected pipe sizes and lengths, storm sewer structures, surface improvements, and expected easements needed to complete construction. As boundary survey will not have been completed at the time of schematic design, the easements will be approximated based on available data including GIS and subject to refinement after completion of a boundary survey. Updates to the schematic design based on city requests will be billed hourly under **Item 3.A**. The fee listed is for one schematic design based on one concept. Should the city desire to develop additional concepts into schematic design the cost for each schematic design will incur an additional fee at the original cost.

FEE: $7,000
Lump Sum
Item 3.3B

Item 3.3C Construction Cost Estimate

Greenway will utilize available data from previous projects and bids to develop a construction cost estimate. A 33% contingency will be included in all estimates to assist with minimizing cost overruns and pricing increases over the future years on future selected projects. Due to the uncertainty of final contractor pricing Greenway cannot guarantee the accuracy of estimates. Timing of projects and market conditions at the time of individual bids play significant roles on final project cost. The fee listed is per cost estimate and additional cost estimates will incur an additional fee.

FEE: $1,500
Lump Sum
Item 3.3C

Deliverables for Part 3

1. Concept plan schematics(s) for resolution of individual drainage concern.
2. Schematic design following approval of concept.
3. Cost estimate based on schematic design.

Part 3 – Project Support

Item 3.A Project Coordination, Client Coordination, Meetings

This item will consist of project coordination of tasks necessary to complete the scope as listed herein, project coordination with the city, team meetings, as necessary throughout the evaluation process. This task will include any coordination with city departments, private dry utility providers, support coordination with city or other subconsultant activities. Time also is included to provide any meeting time for discussions with commissions, committees, council or public as requested by the city. Due to the uncertainties in the amount of work necessary for this we will complete this work hourly. We have provided an estimate to use for budgeting purposes based on anticipated work levels for this stage of the process. Should work approach the estimate and tasks are still remaining for completion, we will coordinate with the City for an addendum to complete the work.

FEE: Hourly, **Item 3.A**

Item 3.B Prints, Federal Express, Deliveries, Mailings, Etc.

Prints, Federal Express charges, deliveries via internal or external courier service, and mailing costs for plans, exhibits, and reports, to include those charged by Greenway's subconsultants, will be billed to you on a time and materials basis in addition to the fees specified in the task items above. Greenway staff time associated with print/compilation development, hand deliveries, and related services will be billed per the current Hourly Rate Schedule in addition to the cost of prints/compilations as specified per the current Reimbursable Rate Schedule. If the Client has an account established with a local printing and/or courier company, Greenway can coordinate print/compilation development and/or deliveries with that company, who will bill you directly for associated costs.

FEE: Per Hourly and Reimbursable Rate Schedules

Item 3.B

ADDITIONS/REVISIONS/EXCLUSIONS

The fees listed above are in effect from the date on this proposal until 60 days thereafter. If the proposal has not been executed within the 60 days, Greenway has the right to reevaluate scope and associated fees and present the Client with an updated proposal. Upon contract ratification, a percentage increase in fees may be applied for contract durations over 12 months.

Greenway also reserves the right to obtain an adjustment in the fee due to changes in the scope of services not provided for herein and outside our control and beyond our view. Our proposal is predicated on the exhibits and information presented to us and the applicable ordinances and regulations in effect and as interpreted by agency staff as of the date of this proposal. Any modifications to the scope of the project which require Greenway to perform additional work will be billed on an hourly basis or a lump sum fee, as agreed upon by the Client.

Any other work not specifically stated herein is excluded from the scope of this proposal. Additionally, all application fees required for submittal or processing any Items identified in this proposal will be the responsibility of the Client.

We understand that in the preparation of this scope of services, we will have assistance (if necessary) from the Client(s)/developer's consultants, i.e., architect, mechanical engineer, electrical engineer, structural engineer, soils or geotechnical engineer, soils testing laboratory, underground utility location specialist, and an attorney if necessary. Greenway shall be held harmless from errors or omissions by these consultants.

CANCELLATION

Greenway Engineering, Inc. (hereinafter Greenway) or the Client may terminate this contract for cause or convenience. However, the party that intends to cancel the contract must do so by giving the other party thirty days (30) notice and must provide their intention to cancel in writing. In the event of contract cancellation, Greenway will be compensated for all reasonable and substantiated costs incurred through close of business on the date of effective date of termination. Greenway will provide the Client with a final invoice within 30 days of the effective date of cancellation. Payment to Greenway must follow ***"Payment/Collections/Interest"*** clause cited within this contract.

SCHEDULE

Greenway will complete each step of the design process as quickly as possible but cannot guarantee any completion schedule due to the variability of the process. Data and design directive points need to be provided to Greenway in a timely manner to ensure a quicker design process. Input from the owner, architect, general contractor and government agencies all affect the timeline. We are currently seeing a three-to-four-month delay on engineering design. We make our best effort to complete these tasks as soon as time is available but make no guarantee on a delivery date.

PAYMENT/COLLECTIONS/INTEREST

Payment is due 30 days from the invoice date unless prior written arrangements have been made. Account balances past 30 days of invoice date are considered "delinquent accounts" and are subject to interest accruing on the past due amounts at a rate of 18% per annum from the date(s) such balance(s) is/are 30 days past due. Should default of any or all payments occur related to the agreed services in this proposal and the account is referred to "collections," it will then be your obligation to pay all collection costs, including, but not limited to, court costs, reasonable attorney's fees equal to 100% of the balance due, lien fees, and collection company fees, accrued interest and any other costs incurred for the collection of this debt.

If you have received an invoice indicating completion of a task item identified in the scope of work herein but have not received the deliverable(s) associated with said task item, you are obligated to contact us to confirm completion status and request receipt of the deliverable(s). You must make such contact within 30 days of receiving the invoice indicating task item completion. We will provide the completed deliverable(s) in the format specified in the task item description or, if not specified, in a mutually agreed upon format.

Payment should be sent to 151 Windy Hill Lane, Winchester, Virginia 22602.

We reserve the right to stop services and withhold the issuance of documents for delinquent accounts. Services and the issuance of documents will resume when delinquent accounts are made current.

We appreciate the opportunity to submit this proposal. Please contact me should you have any questions or wish to change the scope of services.

Sincerely,
Greenway Engineering, Inc.

13 Oct 2026	*13Oct2026*
Randy L. Kepler, PE — Date	Zach Judy, PE, CFM — Date
Director of Engineering	Project Manager

***Signatures Continue on following page:**

APPROVAL SIGNATURE

Signature of representative responsible for payment of services is required for execution of the contract. The scope of services and terms of this proposal are accepted:

_____

Print Authorized Representative Responsible for Payment of Services Name and Title

_____

Signature of Authorized Representative Responsible for Payment of Services Date

BILLING INFORMATION

The following information is required for execution of the contract.

Verification of Land Ownership

Legal Property Owner: _____

Company: _____

Address: _____

Contact No.: _____

Email: _____

Responsible Billing Party (if different from landowner)

Responsible Individual: _____

Company: _____

Address: _____

Contact No.: _____

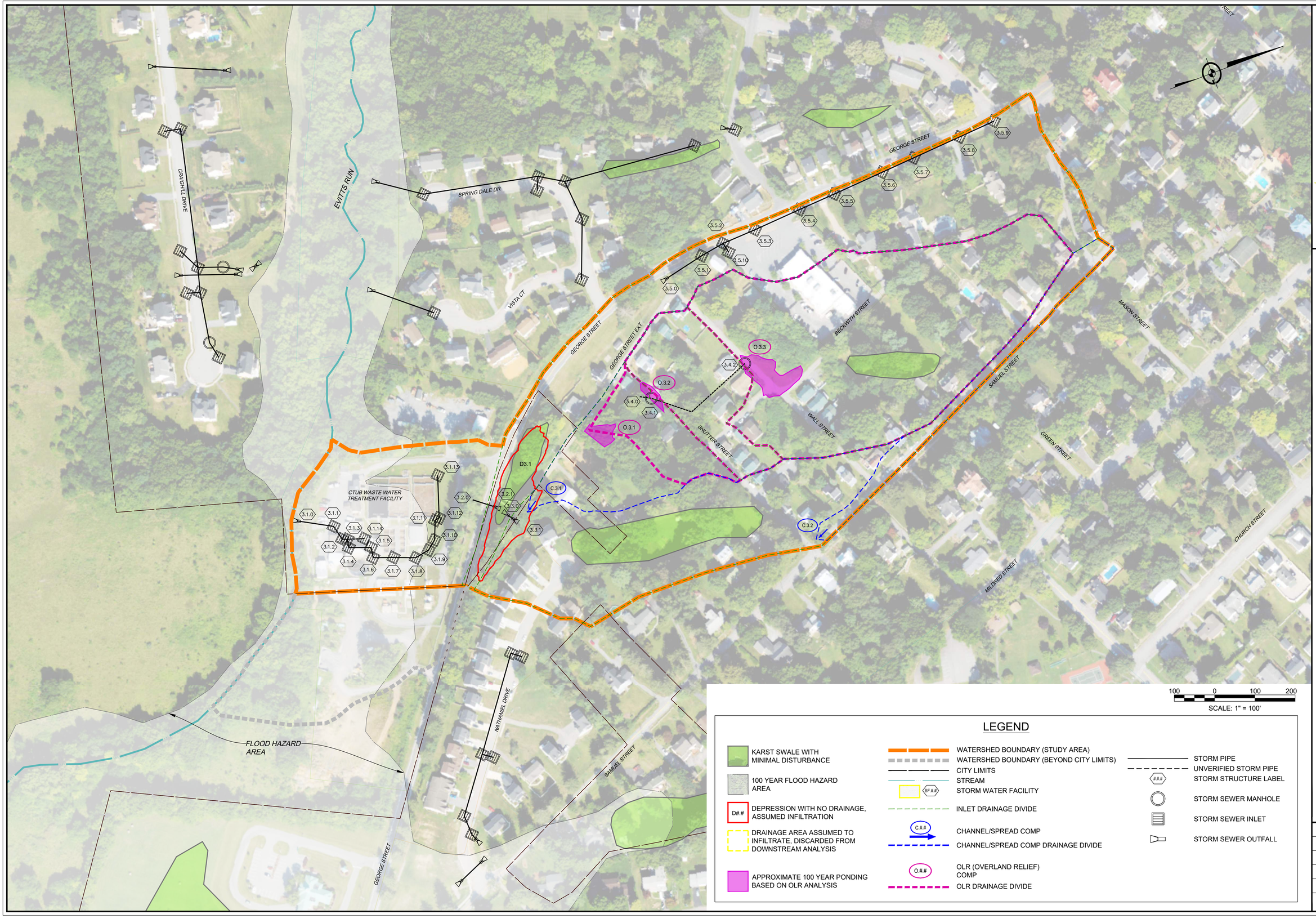
Email: _____

The following information is optional if applicable to your company.

Required Documents

Check below, if any, the documents your company requires for billing purposes.

- ☐ Purchase Order
- ☐ On-site Signed Purchase Order
- ☐ Signed Time Tickets
- ☐ Certification of Insurance
- ☐ W-9
- ☐ Waivers
- ☐ Accounts Payable Registration
- ☐ _____
- ☐ _____
- ☐ _____



100 0 100 200

SCALE: 1" = 100'

LEGEND

- KARST SWALE WITH MINIMAL DISTURBANCE
- 100 YEAR FLOOD HAZARD AREA
- D#.# — DEPRESSION WITH NO DRAINAGE, ASSUMED INFILTRATION
- DRAINAGE AREA ASSUMED TO INFILTRATE, DISCARDED FROM DOWNSTREAM ANALYSIS
- APPROXIMATE 100 YEAR PONDING BASED ON OLR ANALYSIS
- WATERSHED BOUNDARY (STUDY AREA)
- WATERSHED BOUNDARY (BEYOND CITY LIMITS)
- CITY LIMITS
- STREAM
- SF.## — STORM WATER FACILITY
- INLET DRAINAGE DIVIDE
- C.## — CHANNEL/SPREAD COMP
- CHANNEL/SPREAD COMP DRAINAGE DIVIDE
- O.## — OLR (OVERLAND RELIEF) COMP
- OLR DRAINAGE DIVIDE
- STORM PIPE
- UNVERIFIED STORM PIPE
- ### — STORM STRUCTURE LABEL
- STORM SEWER MANHOLE
- STORM SEWER INLET
- STORM SEWER OUTFALL

704 Foxcroft Avenue
Martinsburg, West Virginia 25401
Telephone: (304) 620-5111
Fax: (540) 722-9528
www.greenwayeng.com

GREENWAY ENGINEERING
PROUDLY SERVING WEST VIRGINIA & VIRGINIA
OFFICES IN: MARTINSBURG, WV WINCHESTER, VA & ASHBURN, VA

WATERSHED 3 H&H ANALYSIS EXHIBIT

CITY OF CHARLES TOWN WATERSHEDS

CITY OF CHARLES TOWN - JEFFERSON COUNTY, WEST VIRGINIA

Date:	04/08/2026
Scale:	1" = 100'
Designed By:	ZJ/RLK/ZS
File No.	7037
Sheet	1 Of 1

GREENWAY ENGINEERING

FND 1971

HOURLY RATE SCHEDULE 2026

ENGINEERING	
President, Vice President, Principal	$300 - $250
Professional Engineer VII	$215
Professional Engineer VI	$205
Professional Engineer V	$195
Professional Engineer IV	$185
Professional Engineer III	$175
Professional Engineer II	$165
Professional Engineer I	$155
Senior Engineer VII	$205
Senior Engineer VI	$195
Senior Engineer V	$185
Senior Engineer IV	$175
Senior Engineer III	$165
Senior Engineer II	$155
Senior Engineer I	$145
Engineer VIII	$135
Engineer VII	$125
Engineer VI	$115
Engineer V	$105
Engineer IV	$95
Engineer III	$85
Engineer II	$75
Engineer I	$65
PLANNING	
Senior Planner/Professional Planner V	$205
Senior Planner/Professional Planner IV	$195
Senior Planner/Professional Planner III	$185
Senior Planner/Professional Planner II	$175
Senior Planner/Professional Planner I	$165
Planner VI	$155
Planner V	$145
Planner IV	$135
Planner III	$125
Planner II	$115
Planner I	$105
ENVIRONMENTAL	
Certified Environmental Scientist V, AOSE	$165
Certified Environmental Scientist IV, AOSE	$155
Certified Environmental Scientist III, AOSE	$145
Certified Environmental Scientist II, AOSE	$135
Certified Environmental Scientist I, AOSE	$125
Environmental Scientist VII	$125
Environmental Scientist VI	$115
Environmental Scientist V	$105
Environmental Scientist IV	$95
Environmental Scientist III	$85
Environmental Scientist II	$75
Environmental Scientist I	$65
SURVEYING	
Certified Land Surveyor III	$175
Certified Land Surveyor II	$165
Certified Land Surveyor I	$155
Land Surveyor VIII	$145
Land Surveyor VII	$135
Land Surveyor VI	$125
Land Surveyor V	$115
Land Surveyor IV	$105
Land Surveyor III	$95
Land Surveyor II	$85
Land Surveyor I	$75

Expert Witness will be provided at 1.5 times the regular billing rate.

The rates appearing in this Schedule are accurate and effective as of January 1,2026. Service charges are subject to change at any time and upon occurrence, notification will be given at time of new work request from client.

GREENWAY ENGINEERING

REIMBURSABLE RATE SCHEDULE 2026

PRINT TYPE	
8 ½ x 11 Black and White	$0.15
8 ½ x 14 Black and White	$0.20
11 x 17 Black and White	$0.25
18 x 24 Black and White	$3.00
24 x 36 Black and White	$4.00
30 x 42 Black and White	$5.00
36 x 48 Black and White	$6.00
8 ½ x 11 Color	$0.50
8 ½ x 14 Color	$0.70
11 x 17 Color	$1.00
24 x 36 Color	$15.00
30 x 42 Color	$25.00
18 x 24 Mylar	$10.00
24 x 36 Mylar	$15.00
30 x 42 Mylar	$25.00

COMPILATIONS	
Computer Disk	$15.00
USB Flash Drive	$15.00
Spiral Bound Binder	$7.00
This price is strictly for the binder and does not include the price of the individual prints	
3-Hole Binder	$15.00
This price is strictly for the binder and does not include the price of the individual prints	

COURIER SERVICE	
Berkeley & Jefferson County Areas	$25.00
Frederick County & Winchester City Areas	$30.00
Clarke, Warren, Loudoun & Shenandoah County Areas	$35.00
Overnight and other area deliveries are available and billed on a per usage basis.	

Prints, Federal Express charges, deliveries and mailing costs for plans, exhibits and reports will be billed to you as ordered in addition to any contracted or quoted fees. Large submittals will be sent out to our printing company and will be billed with an additional 15% to you as needed. If you have an account setup with a local printing company, we can have that company bill you directly for these printing costs.

All travel costs (mileage, lodging, meals, etc.) are on a per diem basis.

Subcontractual services are billed with a 15% markup.

The rates appearing in this Schedule are accurate and effective as of January 1, 2026. Service charges are subject to change at any time and upon occurrence, notification will be given at time of new work request from client.

If you have any questions or require current rate and fee information on your account(s), please contact our accounting department at (540) 662-4185.

Appendix-Watershed 3

Watershed 3 consists of areas draining to Evitts Run around and through the CTUB wastewater treatment plan. Small portions of the watershed drain as sheet flow directly adjacent to the stream and majority of the drainage shed concentrates at the culvert inlet adjacent to the treatment plant across George Street (3.1.1). It was noted that two houses have been constructed within the past five years in a location with significant drainage implications. These are described further in relation to the overland relief analysis. No suspected stormwater management facilities were identified within watershed 3.

Storm Sewer and Culverts

The storm sewer and culvert infrastructure within watershed 3 consists of five individual storm sewer systems/culverts.

System 1 provides drainage around the CTUB wastewater treatment plant. This system is not analyzed as the only impacts due to lack of capacity would be wholly within the CTUB property. It is expected that the system has an engineered design, although the only documents provided by CTUB consist of a layout showing the storm system. The system discharges directly to Evitts Run.

System 2 consists of a culvert across George Street. The outfall for this culvert appears to have been buried and/or collapsed. Little evidence of overtopping of George Street exists due to this collapse exists.

System 3 is the culvert providing drainage across South George Street Extension. The culvert is severely undersized for the drainage area.

System 4 consists of grate inlets along Wall Street and Shutter Street. The outfall for this system is buried and during rain events the system discharges through the grate inlet on Shutter Street.

System 5 provides drainage along George Street and was installed with construction of the municipal building housing CTUB and the Charles Town Police Department. This system was not analyzed as it was installed per an engineered design.

Channel/Roadway Spread Analysis

No significant open space channels were identified within watershed 3 other than the two karst swales and the channel between George Street and George Street Extension. These were not analyzed as they all appear to have significant infiltration and/or capacity.

Two locations were analyzed for their potential issues resulting from channel flow. The table below lists the issues.

Identifier	Location	Description
C.3.1	George Street Ext	Roadside ditch
C.3.2	Samuel Street	Spread

Depressions

One significant infiltration depression was identified within watershed 3. D3.1 does have a previously installed outlet which is the culvert under George Street(3.2). The outfall for the culvert appears to be buried. Little evidence of significant overtopping of George Street or erosion of its roadside ditch seems to indicate this low-lying area infiltrates significantly through natural process and through the buried outfall 3.2.0.

Overland Relief

The majority of watershed 3's issues were analyzed utilizing overland relief analyses.

The issue associated with O.3.1 was created by the construction of two houses at 815 and 817 George Street Extension. The houses were constructed within a drainage swale with little to no consideration for functional drainage. Over 10 acres drained through the swale that was cut off by the construction. A depression now exists both within the lot of the more upstream of the new houses and the neighboring lot that had an existing residence. The depression must fill before spilling into the street. The foundation of 813 George Street Extension is inundated by this ponding even during smaller events.

O.3.2 and O.3.3 are associated with potential impacts to local roadways and several residences. O3.3 has an inlet and storm sewer, but the routing from 3.4.2 to 3.3.1 is unclear and the original outfall seems to have been buried. The system discharges through the grate at 3.3.1. 3.4.2 is also located outside the true low point resulting in inundation even during smaller events.

CITY OF CHARLES TOWN WATERSHEDS

WATERSHED 3 H&H ANALYSIS EXHIBIT

CITY OF CHARLES TOWN - JEFFERSON COUNTY, WEST VIRGINIA

704 Foxcroft Avenue
Martinsburg, West Virginia 25401
Telephone: (304) 620-5111
Fax: (540) 722-9528
www.greenwayeng.com

GREENWAY ENGINEERING
PROUDLY SERVING WEST VIRGINIA & VIRGINIA
OFFICES IN: MARTINSBURG, WV WINCHESTER, VA & ASHBURN, VA

Date:	04/08/2026
Scale:	1" = 100'
Designed By:	ZJ/RLK/ZS
File No.	7037
Sheet	1 Of 1

100 0 100 200
SCALE: 1" = 100'

LEGEND

- KARST SWALE WITH MINIMAL DISTURBANCE
- 100 YEAR FLOOD HAZARD AREA
- D#.# — DEPRESSION WITH NO DRAINAGE, ASSUMED INFILTRATION
- DRAINAGE AREA ASSUMED TO INFILTRATE, DISCARDED FROM DOWNSTREAM ANALYSIS
- APPROXIMATE 100 YEAR PONDING BASED ON OLR ANALYSIS
- WATERSHED BOUNDARY (STUDY AREA)
- WATERSHED BOUNDARY (BEYOND CITY LIMITS)
- CITY LIMITS
- STREAM
- SF.## — STORM WATER FACILITY
- INLET DRAINAGE DIVIDE
- C.## — CHANNEL/SPREAD COMP
- CHANNEL/SPREAD COMP DRAINAGE DIVIDE
- O.## — OLR (OVERLAND RELIEF) COMP
- OLR DRAINAGE DIVIDE
- STORM PIPE
- UNVERIFIED STORM PIPE
- ### — STORM STRUCTURE LABEL
- STORM SEWER MANHOLE
- STORM SEWER INLET
- STORM SEWER OUTFALL

Roadside Ditch and Roadway Spread Analysis

Watershed 3

												2 Year						10 Year						100 Year					
												2yr Karst Factor			0.69			10yr Karst Factor			0.77			100yr Karst Factor			0.83		
Identifier	Location	Description	Side Slope 1 (H ft:1 ft)	Side Slope 2 (H ft:1 ft)	Upstream Road Length(ft)	Upstream Intersections	Available Depth for Ditch/Gutter(ft)	Available Width for Spread (ft)	Approximate Running Slope (%)	Drainage Area (Acre)	C Factor	Tc (Min)	Rainfall Intensity (in/hr)	Flow (cfs)	Depth of flow (ft)	Roadway Surcharge (ft)	Spread (ft)	Travel Lane Spread (ft)	Rainfall Intensity (in/hr)	Flow (cfs)	Depth of flow (ft)	Roadway Surcharge (ft)	Spread (ft)	Travel Lane Spread (ft)	Rainfall Intensity (in/hr)	Flow (cfs)	Depth of flow (ft)	Roadway Surcharge (ft)	Spread (ft)	Travel Lane Spread (ft)
C.3.1	George Street Ext	Roadside ditch	20	3	550	0	0.25	0	4%	11.48	0.58	20	2.72	12.50	0.49	0.24	12.00	Full	3.77	19.33	0.57	0.32	16.00	Full	5.33	29.46	0.67	0.42	21.00	Full
C.3.2	Samuel Street	Spread	NA	NA	1000	2	0	3	2%	0.83	0.49	5	4.73	1.33	0.14	0.14	7.04	5.04	6.52	2.05	0.17	0.17	8.29	6.29	9.23	3.12	0.19	0.19	9.71	7.71

NOTES

For roadside ditches available depth is the approximated depth of the ditch outside the roadway, 0.1' is indicative of no defined roadside ditch

For spread comps available depth of 0' is indicative of no gutter pan and 0.1' is indicative of a gutter pan

For spread comps a negative available spread is indicative of a local depression that results in an initial spread for all storm events

Upstream Intersections within 500ft of the highpoint are excluded from the upstream intersection counts

Available width is the approximated area available for spread outside an assumed 10ft travel lane

Roadway surcharge depth is the expected depth of water at the edge of pavement

Mannings n assumptions; ditch/channel = 0.025; road/gutter spread = .016

Road cross slopes assumed at 2%

Overland Relief Analysis (OLR)

Watershed 3

										10 Year								100 Year							
										10yr Karst Factor					0.77			100yr Karst Factor					0.83		
Identifier	Location	Constraint Description	Approximated Weir Elevation	Inlets Present	Throat Inlet or 2 Grates Present	Storm sewer capacity (cfs)	Drainage Area (Acre)	C Factor	Tc (Min)	Rainfall Intensity (in/hr)	OLR Flow (cfs)	Depth (ft)	Approximated WSE	Buildings Impacted	Local Roadway Inundation (ft)	Primary Route Inundation (ft)	Singular Access Point Impacts	Rainfall Intensity (in/hr)	OLR Flow (cfs)	Depth (ft)	Approximated WSE	Buildings Impacted	Local Roadway Inundation (ft)	Primary Route Inundation (ft)	Singular Access Point Impacts
O.3.1	George Street Ext	Houses/Yards	493.00	0	No	0.00	10.28	0.58	20	3.77	17.31	0.69	493.69	2	0	0	No	5.33	26.38	0.80	493.80	2	0	0	No
O.3.2	Shutter Street	Roadway	501.00	1	No	0.00	9.35	0.59	15	4.18	17.76	0.21	501.21	1	50	0	No	5.84	26.74	0.27	501.27	1	75	0	No
O.3.3	Wall Street	Houses/Yards	512.10	1	No	0.00	7.63	0.58	15	4.18	14.24	0.41	512.51	2	220	0	No	5.84	21.45	0.64	512.74	2	240	0	No

NOTES

Weir coefficient assumed as 3.27

OLR flow accounts for storm sewer capacity where redundant inlets are present to ensure drainage

Storm sewer capacity is only accounted for were either throat inlets or redundant grate inlets are present within the 100 year ponding area

Storm Sewer Pipe Analysis

Watershed 3

																						2 Year					10 Year				
																						2yr Karst Factor				0.69	10yr Karst Factor				0.77
Inlet/Structure Name	**Downstream Structure**	**Structure Type**	**Inlet Size (in)**	**Inlet Profile**	**Approximate Top Elevation/Invert**	**Approximate Invert Up**	**Approximate Invert Down**	**Pipe Length (ft)**	**Pipe Material**	**Pipe Size (in)**	**Approximate Pipe Slope (%)**	**Pipe Mannings 'n'**	**Flow Area (ft^2)**	**Hydraulic Radius**	**Full Flow Capacity (cfs)**	**Inlet C Factor**	**Inlet Drainage Area (Acres)**	**Time to Inlet (min)**	**System C Factor**	**System Drainage Area (Acre)**	**System Time (Min)**	**Inlet Rainfall Intensity (in/hr)**	**Flow To Inlet (cfs)**	**System Rainfall Intensity (in/hr)**	**System Flow (cfs)**	**System Flow/Pipe Full Flow (%)**	**Inlet Rainfall Intensity (in/hr)**	**Flow To Inlet (cfs)**	**System Rainfall Intensity (in/hr)**	**System Flow (cfs)**	**System Flow/Pipe Full Flow (%)**
3.1.14	3.1.3	Grate	24 x 24	Private System, Engineered Design, Not Evaluated																											
3.1.13	3.1.12	Grate	24 x 24																												
3.1.12	3.1.11	Grate	24 x 24																												
3.1.11	3.1.10	MH																													
3.1.10	3.1.9	MH																													
3.1.9	3.1.8	Grate	24 x 24																												
3.1.8	3.1.7	Grate	24 x 24																												
3.1.7	3.1.6	Grate	24 x 24																												
3.1.6	3.1.5	Grate	24 x 24																												
3.1.5	3.1.4	Grate	24 x 24																												
3.1.4	3.1.3	Grate	24 x 24																												
3.1.3	3.1.2	Grate	24 x 24																												
3.1.2	3.1.1	Grate	24 x 24																												
3.1.1	3.1.0	Grate	24 x 24																												
3.1.0		Outlet																													
3.2.1	3.2.0	Culvert Inv		Sag	480.00	480.00			Concrete	24						0.55	24.08	20	0.55	24.08	20	3.36	30.70	3.36	30.70		4.59	46.81	4.59	46.81	
3.2.0		Outlet			Buried																										
3.3.1	3.3.0	Culvert Inv		Sag	481.28	481.28	480.25	24	Concrete	15	4.3%	0.013	1.23	0.31	13.42	0.55	17.18	20	0.55	17.18	20	3.36	21.91	3.36	21.91	163%	4.59	33.40	4.59	33.40	249%
3.3.0		Outlet			480.25																										
3.4.2	3.4.1	Grate	30 x 30	Sag	505.05	502.05	497	283	PVC	12	1.8%	0.012	0.79	0.25	5.19	0.58	7.63	15	0.58	7.63	15	3.36	10.26	3.36	10.26	198%	4.59	15.64	4.59	15.64	301%
3.4.1	3.4.0	Grate	24 x 24	Sag	500.00	497.00										0.65	1.72	10	0.59	9.35	15	3.04	2.35	3.36	12.85		4.18	3.60	4.59	19.59	
3.4.0		Outlet			Buried																										
3.5.10	3.5.2	Grate	18 x 18	Engineered Design, Not Evaluated																											
3.5.9	3.5.8	Curb Inlet	48																												
3.5.8	3.5.7	Curb Inlet	48																												
3.5.7	3.5.6	Curb Inlet	48																												
3.5.6	3.5.5	Curb Inlet	48																												
3.5.5	3.5.4	Curb Inlet	48																												
3.5.4	3.5.3	Curb Inlet	48																												
3.5.3	3.5.2	Curb Inlet	48																												
3.5.2	3.5.1	Curb Inlet	48																												
3.5.1	3.5.0	Curb Inlet	48																												
3.5.0		Outlet																													

NOTES

Structures assumed to be 3' deep unless direct field observations indicate significant difference

Negative pipe slopes are assumed to have the capacity equivalent to a slope of 0.1%

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2051: Payment of Bills - October 19, 2026

ATTACHMENTS:

- PARKS N REC COUNCIL REPORT 2026-10-19.pdf
- COUNCIL REPORT PCARD 10-19-2026.pdf
- GEN FUND COUNCIL REPORT 2026-10-19.pdf
- CAPITAL RESERVE COUNCIL REPORT 2026-10-19.pdf

Expense Approval Report

Charles Town, WV

By Fund

Post Dates 10/11/2026 - 10/16/2026

Vendor Name	Payable Number	Post Date	Description (Item)	Account Number		Amount
Fund: 207 - PARKS & REC						
Department: 900 - PARKS & REC						
POTOMAC EDISON COMPANY	INV0002915	10/13/2026	Sept 26 JMP Electricity Service	207-900-213		16.62
CBP ENTERPRISES	17027	10/15/2026	Sept 26 Evitts Run Mowing Service	207-900-230		1275.00
CBP ENTERPRISES	17028	10/15/2026	Sept 26 Happy Retreat Mowing Service	207-900-230		1675.00
CBP ENTERPRISES	17029	10/15/2026	Sept 26 Craig Hill Mowing Service	207-900-230		1250.00
CBP ENTERPRISES	17030	10/15/2026	Sept 26 JMP Mowing Service	207-900-230		1550.00
CBP ENTERPRISES	17031	10/15/2026	Sept 26 Willingham Knolls Park Mowing Service	207-900-230		1350.00
					Department 900 - PARKS & REC Total:	**7116.62**
					Fund 207 - PARKS & REC Total:	**7116.62**
					Grand Total:	**7116.62**

Report Summary

Fund Summary

Fund	Payment Amount
207 - PARKS & REC	7116.62
Grand Total:	**7116.62**

Account Summary

Account	Account Name	Payment Amount
207-900-213	UTILITIES	16.62
207-900-230	CONTRACTED SERVICES	7100.00
	Grand Total:	**7116.62**

Project Account Summary

Project Account K	Payment Amount
None	7116.62
Grand Total:	**7116.62**

Authorization Signatures

. COUNCIL MEMBER

. COUNCIL MEMBER

Expense Approval Report

Charles Town, WV

By Fund

Post Dates 9/1/2026 - 9/30/2026

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number		Amount
Fund: 001 - GENERAL FUND						
CHARLES TOWN UTILITY BOAF	INV0002476	09/10/2026	Aug 26 CTUB Water Service	001-114-020		87.00
						87.00
Department: 402 - ECONOMIC DEVELOPMENT						
ADOBE INC	3567449180	09/02/2026	Sept26 Adobe Stock Subscription	001-402-222		29.99
Five Below	INV0002757	09/02/2026	Walk abt Nothing Anniversary Games	001-402-341		9.63
APPLE	INV0002759	09/08/2026	Sept 26 Music Subscription	001-402-222		21.35
SUNOCO	INV0002798	09/09/2026	Fuel 9/8 WV Mainstreet Conference	001-402-214		45.54
TOWN MART CITGO	INV0002799	09/09/2026	Fuel 9/7 WV Mainstreet Conference	001-402-214		44.36
Taqueria 84	INV0002758	09/10/2026	Lunch 9/9 WV Mainstreet Conference	001-402-214		11.77
Backyard Pizza & Raw Bar	INV0002800	09/10/2026	9/08 Dinner WV Mainstreet Conference	001-402-214		17.42
SHEETZ	INV0002801	09/11/2026	Fuel 9/18 WV Mainstreet Conference	001-402-214		38.22
					Department 402 - ECONOMIC DEVELOPMENT Total:	**218.28**
Department: 410 - CITY COUNCIL						
JEFFERSON COUNTY CHAMBE	10852	09/03/2026	Ricketts Luncheon State of the Towns 26	001-410-221		28.00
					Department 410 - CITY COUNCIL Total:	**28.00**
Department: 413 - TREASURER'S OFFICE						
JEFFERSON PUBLISHING COMI	74554	09/02/2026	8/20 Accounting Clerk I Job Posting	001-413-220		69.50
JEFFERSON PUBLISHING COMI	74555	09/02/2026	8/27 Accounting Clerk I job Posting	001-413-220		69.50
JEFFERSON PUBLISHING COMI	74671	09/15/2026	RFP CPA for Finance Procedures&Policies Ma	001-413-220		25.90
					Department 413 - TREASURER'S OFFICE Total:	**164.90**
Department: 417 - CITY ATTORNEY						
West Virginia State Bar	INV0002865	09/01/2026	CA WV Bar Membership Renewal	001-417-222		455.00
JACQUELINE C SHADLE, COUN	INV0002866	09/17/2026	Record Search for Perry Annexation	001-417-341		15.50
THOMSON REUTERS	0854078013	09/25/2026	Sept 26 Legal Research Subscription	001-417-222		444.19
					Department 417 - CITY ATTORNEY Total:	**914.69**
Department: 425 - ENFORCEMENT AGENCY						
DAYS INN	INV0002775	09/14/2026	CE WV COA Hotel Nights 9/9-11	001-425-214		210.75
AMAZON	INV0002776	09/22/2026	CE Ergonomic Mouse& Keyboard	001-425-341		169.99
					Department 425 - ENFORCEMENT AGENCY Total:	**380.74**
Department: 436 - BUILDING INSPECTION						
DAYS INN	INV0002774	09/14/2026	BI WV COA Fall Training Hotel Nights 9/9-11	001-436-214		225.90
MATTHEW ANDERSON, PE, PL	25700	09/15/2026	9/10-11 Residential Inspections	001-436-223		1000.00
VERIZON WIRELESS	6152754472	09/17/2026	July&Aug 26 BI Hotspot	001-436-211		40.04

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number	Amount
MATTHEW ANDERSON, PE, PL	25727	09/29/2026	9/23 & 24 Residential Inspections	001-436-223	1000.00
				Department 436 - BUILDING INSPECTION Total:	**2265.94**
Department: 437 - PLANNING & ZONING					
JEFFERSON PUBLISHING COMI	74672	09/15/2026	NPH TXA26-01 Zng Ord Amndment	001-437-220	35.10
JEFFERSON PUBLISHING COMI	74716	09/17/2026	NPH COA 26-13 206 W Wash & FIP 26-03 202	001-437-220	36.94
Borough of Gettysburg	INV0002760	09/17/2026	9/17 Parking ICMA Training	001-437-214	18.00
Borough of Gettysburg	INV0002761	09/17/2026	9/18 Parking ICMA Training	001-437-214	21.00
Best Ice Cream & Smoothies	INV0002762	09/17/2026	9/16 Dinner ICMA Training	001-437-214	7.00
City Mart	INV0002763	09/17/2026	9/16 Drink ICMA Training	001-437-214	2.64
Hotel Gettysburg	INV0002764	09/18/2026	Lunch 9/16 ICMA Training	001-437-214	21.20
TOWN MART CITGO	INV0002765	09/18/2026	CH Explorer Fuel 9/16 ICMA Training	001-437-214	32.82
STARBUCKS	INV0002766	09/18/2026	9/18 Breakfast ICMA Training	001-437-214	6.41
Hotel Gettysburg	INV0002767	09/21/2026	9/17 Dinner ICMA Training	001-437-214	37.10
Hotel Gettysburg	INV0002768	09/21/2026	Hotel Nights 9/16-18 ICMA Training	001-437-214	441.78
SUNOCO	INV0002769	09/21/2026	CH Explorer Fuel 9/18 ICMA Training	001-437-214	41.19
Hotel Gettysburg	INV0002770	09/21/2026	9/17 Coffee ICMA Training	001-437-214	6.10
Hotel Gettysburg	INV0002771	09/21/2026	9/17 Breakfast ICMA Training	001-437-214	12.72
Hotel Gettysburg	INV0002772	09/21/2026	9/16 Coffee ICMA Training	001-437-214	6.94
ADOBE INC	3588682917	09/23/2026	FY 27 Adobe Express Subscription	001-437-222	105.99
JEFFERSON PUBLISHING COMI	74785	09/24/2026	NPH SLD 26-03 Prospect Place	001-437-220	35.10
				Department 437 - PLANNING & ZONING Total:	**868.03**
Department: 440 - CITY HALL					
PATTON BUILDING SERVICES I	138414	09/02/2026	Aug 26 CH Cleaning Services	001-440-230	933.50
PATTON BUILDING SERVICES I	138414	09/02/2026	Aug 26 CWH Cleaning Services	001-440-230	125.00
PITNEY BOWES GLOBAL FINAN	3323133061	09/03/2026	1st Qrtr FY 27 Postage Machine Lease	001-440-219	505.23
ZOOM.US	368805274	09/07/2026	Sept 26 Online Meeting Subscription	001-440-222	52.43
STAPLES ADVANTAGE INC	7686709524	09/07/2026	CH Register Rolls&Correctn Tape&AA Batterie	001-440-341	70.06
CHARLES TOWN UTILITY BOAF	INV0002476	09/10/2026	Aug 26 RH Water Service	001-440-213	94.68
CHARLES TOWN UTILITY BOAF	INV0002476	09/10/2026	Aug 26 CH Water Service	001-440-213	178.01
COMCAST CORPORATION	INV0002520	09/10/2026	Sept 26 CWHall Internet Service	001-440-213	153.85
AMAZON	INV0002830	09/10/2026	CH FY 27 Prime Membership	001-440-222	129.00
ENVIRO-TECH PEST SERVICES	496651	09/11/2026	Sept26 CH Pest Service	001-440-230	77.04
STAPLES ADVANTAGE INC	7687501063	09/21/2026	CH Paper Reams X 3	001-440-341	135.72
AMAZON	INV0002652	09/22/2026	CH 3rd Flr Water Dispenser Replacement	001-440-341	85.45
SHENTEL BUSINESS	INV0002676	09/24/2026	Oct 26 CH & PD Internet Service	001-440-213	950.00
US POSTAL SERVICE	INV0002696	09/29/2026	CH Stamp Booklet	001-440-218	16.40
PITNEY BOWES GLOBAL FINAN	INV0002690	09/30/2026	Postage Machine Cartridges X 2	001-440-218	322.02
PITNEY BOWES GLOBAL FINAN	INV0002691	09/30/2026	Postage Machine Ink Cartridge X 1	001-440-218	161.01
				Department 440 - CITY HALL Total:	**3989.40**
Department: 571 - PARKING					
HOME DEPOT INC	INV0002882	09/02/2026	Parking Quick Link X 2	001-571-341	17.08
AMAZON	INV0002875	09/08/2026	Parking AA Batteries X 24	001-571-341	17.23
AMAZON	INV0002877	09/21/2026	Parking Battery Holders	001-571-341	22.47

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number		Amount
AMAZON	INV0002879	09/22/2026	Parking AA Batteries x 2 Packs	001-571-341		25.90
					Department 571 - PARKING Total:	**82.68**
Department: 700 - POLICE DEPARTMENT						
SHEETZ	INV0002480	09/01/2026	Car#18 Fuel 08/31	001-700-343		42.00
7-ELEVEN	INV0002484	09/01/2026	Car#14 Fuel 08/31	001-700-343		80.50
PATTON BUILDING SERVICES I	138414	09/02/2026	Aug 26 PD Cleaning Services	001-700-230		933.50
SHEETZ	INV0002481	09/02/2026	Car#18 Fuel 09/01	001-700-343		47.00
SHEETZ	INV0002483	09/02/2026	Car#17 Fuel 09/01	001-700-343		51.00
MARTINS FUEL	INV0002486	09/02/2026	Car#15 Fuel 09/01	001-700-343		55.70
BP	INV0002487	09/02/2026	Car#7 Fuel 09/01	001-700-343		64.50
TOWN MART CITGO	INV0002488	09/02/2026	Car#11 Fuel 08/31	001-700-343		55.55
TRANSUNION	6707023-20260	09/03/2026	Aug 26 Investigative Subscription	001-700-222		110.00
BP	INV0002478	09/03/2026	Car#4 Fuel 09/02	001-700-343		83.38
SHEETZ	INV0002479	09/03/2026	Car#29 Fuel 9/02	001-700-343		38.17
SHEETZ	INV0002482	09/03/2026	Car#18 Fuel 09/02	001-700-343		44.00
SHEETZ	INV0002485	09/03/2026	Car#14 Fuel 9/02	001-700-343		71.74
MAGNET FORENSICS	SIN097245	09/03/2026	FY27 Digital Forensics Platform Subscription	001-700-353		11745.00
ENVIRO-TECH PEST SERVICES	496354	09/04/2026	Sept 26 661 S George Pest Service	001-700-230		91.49
SHEETZ	INV0002505	09/04/2026	Car#10 Fuel 09/03	001-700-343		62.68
SHEETZ	INV0002508	09/04/2026	Car#17 Fuel 09/03	001-700-343		37.00
SHEETZ	INV0002509	09/04/2026	Car#17 Fuel 09/03	001-700-343		79.00
7-ELEVEN	INV0002511	09/04/2026	Car#14 Fuel 09/03	001-700-343		54.00
BP	INV0002513	09/04/2026	Car#3 Fuel 09/02	001-700-343		86.02
TOWN MART CITGO	INV0002518	09/04/2026	Car#11 Fuel 09/02	001-700-343		70.70
EXXON MOBILE	INV0002499	09/07/2026	Car#27 Fuel 09/04	001-700-343		57.09
LIBERTY GET N GO	INV0002500	09/07/2026	Car#29 Fuel 09/06	001-700-343		41.28
7-ELEVEN	INV0002501	09/07/2026	Car#29 Fuel 09/04	001-700-343		54.57
SHEETZ	INV0002502	09/07/2026	Car#18 Fuel 09/06	001-700-343		40.00
PILOT	INV0002503	09/07/2026	Car#21 Fuel 09/04	001-700-343		47.49
7-ELEVEN	INV0002504	09/07/2026	Car#21 Fuel 09/05	001-700-343		48.10
SHEETZ	INV0002506	09/07/2026	Car#10 Fuel 09/05	001-700-343		22.34
LIBERTY GET N GO	INV0002507	09/07/2026	Car#25 Fuel 09/03	001-700-343		60.35
SHEETZ	INV0002510	09/07/2026	Car#17 Fuel 09/5	001-700-343		66.28
LIBERTY GET N GO	INV0002512	09/07/2026	Car#12 Fuel 09/03	001-700-343		75.48
BP	INV0002514	09/07/2026	Car#3 Fuel 090/02	001-700-343		63.89
SHEETZ	INV0002515	09/07/2026	Car#26 Fuel 09/04	001-700-343		36.55
SHEETZ	INV0002516	09/07/2026	Car#26 Fuel 09/03	001-700-343		44.86
MARTINS FUEL	INV0002517	09/07/2026	Car#15 Fuel 09/05	001-700-343		44.41
TIMOTHY R. CROSS	INV0002870	09/07/2026	Car#6 Detailing	001-700-217		180.00
ROCS	INV0002871	09/07/2026	Car#28 Fuel 09/03	001-700-343		44.01
FACEBOOK.COM	INV0002872	09/07/2026	9/4 Recruitment Ad Boost	001-700-220		2.00
FACEBOOK.COM	INV0002873	09/07/2026	9/5 Recruitment Ad Boost	001-700-220		2.00
ROCS	INV0002883	09/07/2026	Car#1 Fuel 9/03	001-700-343		91.39

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number	Amount
BATTERY MART	INV0002884	09/07/2026	Car#6 Battery	001-700-217	199.95
BP	INV0002522	09/08/2026	Car#4 Fuel 09/07	001-700-343	78.13
SHEETZ	INV0002523	09/08/2026	Car#18 Fuel 09/07	001-700-343	33.00
SHEETZ	INV0002524	09/08/2026	Car#16 Fuel 09/07	001-700-343	34.76
BP	INV0002525	09/08/2026	Car#16 Fuel 09/07	001-700-343	80.24
SHEETZ	INV0002526	09/08/2026	Car#21 Fuel 09/07	001-700-343	42.17
SHEETZ	INV0002527	09/08/2026	Car#25 Fue; 09/07	001-700-343	51.59
SHEETZ	INV0002528	09/08/2026	Car#14 Fuel 09/07	001-700-343	72.01
FACEBOOK.COM	INV0002874	09/08/2026	9/5 Recruitment Ad Boost	001-700-220	2.26
CREAMERS AUTO SERVICE CEI	152292	09/09/2026	Car#12 WV Inspection & Oil Service	001-700-217	18.97
CREAMERS AUTO SERVICE CEI	152292	09/09/2026	Car#12 WV Inspection & Oil Service	001-700-343	115.28
CREAMERS AUTO SERVICE CEI	152307	09/09/2026	Car#7 Oil Service & Headlight Bulb	001-700-217	9.20
CREAMERS AUTO SERVICE CEI	152307	09/09/2026	Car#7 Oil Service & Headlight Bulb	001-700-343	92.28
MUTH RAYMOND	2350	09/09/2026	Car#6 Emergency Light System Repair	001-700-217	603.75
10-42 TACTICAL LLC	8264	09/09/2026	Kutcher & Desarno Armors X 2	001-700-345	3210.00
SHEETZ	INV0002549	09/09/2026	Car#18 Fuel 09/08	001-700-343	33.00
SHEETZ	INV0002550	09/09/2026	Car#25 Fuel 09/08	001-700-343	64.25
SHEETZ	INV0002551	09/09/2026	Car#14 Fuel 09/08	001-700-343	76.50
TOWN MART CITGO	INV0002552	09/09/2026	Car#12 Fuel 09/07	001-700-343	65.31
CHARLES TOWN UTILITY BOAF	INV0002476	09/10/2026	Aug 26 PD Water Service	001-700-213	176.65
BP	INV0002553	09/10/2026	Car#3 Fuel 09/09	001-700-343	85.39
SHEETZ	INV0002554	09/10/2026	Car#18 Fuel 9/09	001-700-343	43.00
SHEETZ	INV0002555	09/10/2026	Car#14 Fuel 09/09	001-700-343	71.00
7-ELEVEN	INV0002556	09/10/2026	Car#26 Fuel 09/09	001-700-343	49.69
LIBERTY GET N GO	INV0002557	09/10/2026	Car#7 Fuel 09/08	001-700-343	85.21
BP	INV0002558	09/10/2026	Car#11 Fuel 09/09	001-700-343	79.79
pearsonplus.com	INV0002885	09/10/2026	Criminal Investigation Promotional Book	001-700-341	94.98
pearsonplus.com	INV0002886	09/10/2026	Law Enforcement in 21st Century Promotiona	001-700-341	94.98
pearsonplus.com	INV0002887	09/10/2026	Organizational Behavior & Mgnt Promotional	001-700-341	94.98
pearsonplus.com	INV0002888	09/10/2026	Police Admin: Structures Processes Promotior	001-700-341	94.98
pearsonplus.com	INV0002889	09/10/2026	Supervision of Police Personnel Promotional E	001-700-341	94.98
CREAMERS AUTO SERVICE CEI	152277	09/11/2026	Car#16 4 Tire Mount& Alignment& Oil Service	001-700-343	335.18
EXXON MOBILE	INV0002565	09/11/2026	Car#27 Fuel 9/10	001-700-343	65.47
SHEETZ	INV0002566	09/11/2026	Car#17 Fuel 09/10	001-700-343	75.00
TOWN MART CITGO	INV0002567	09/11/2026	Car#12 Fuel 09/09	001-700-343	69.16
BP	INV0002753	09/11/2026	Car#3 Fuel 09/10	001-700-343	88.80
AMAZON	INV0002890	09/11/2026	PD Camera Case & Stick	001-700-341	35.15
AMAZON	INV0002891	09/11/2026	PD AAA Batteries	001-700-341	20.28
10-42 TACTICAL LLC	8254	09/14/2026	CALEA Logo X 24	001-700-341	615.33
LIBERTY GET N GO	INV0002609	09/14/2026	Car#29 Fuel 09/10	001-700-343	33.65
SHEETZ	INV0002610	09/14/2026	Car#29 Fuel 09/11	001-700-343	53.17
SHEETZ	INV0002611	09/14/2026	Car#18 Fuel 09/13	001-700-343	29.00
SHEETZ	INV0002613	09/14/2026	Car#21 Fuel 9/13	001-700-343	49.58
MARATHON	INV0002614	09/14/2026	Ca#21 Fuel 9/11	001-700-343	45.42

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number	Amount
SHEETZ	INV0002616	09/14/2026	Car#25 Fuel 09/13	001-700-343	63.14
SHEETZ	INV0002617	09/14/2026	Car#17 Fuel 09/12	001-700-343	85.00
SHEETZ	INV0002619	09/14/2026	Car#26 Fuel 09/11	001-700-343	45.29
7-ELEVEN	INV0002622	09/14/2026	Car#7 Fuel 09/11	001-700-343	77.04
SHEETZ	INV0002892	09/14/2026	Car#1 Fuel 9/12	001-700-343	93.86
AMAZON	INV0002893	09/14/2026	PD Camcorder	001-700-341	783.02
CREAMERS AUTO SERVICE CEN	152401	09/15/2026	Car#6 WV Inspection	001-700-217	18.67
CREAMERS AUTO SERVICE CEN	152404	09/15/2026	Car#7 Oil Service	001-700-343	115.97
CREAMERS AUTO SERVICE CEN	152409	09/15/2026	Car#1 4 New Tires Mount&Balance&Align	001-700-343	235.35
SHEETZ	INV0002612	09/15/2026	Car#18 Fuel 9/14	001-700-343	50.00
GO MART	INV0002615	09/15/2026	Car#21 Fuel 09/13	001-700-343	62.54
SHEETZ	INV0002618	09/15/2026	Car#14 Fuel 09/14	001-700-343	61.01
SHEETZ	INV0002620	09/15/2026	Car#26 Fuel 09/13	001-700-343	46.11
MARTINS FUEL	INV0002621	09/15/2026	Car#15 Fuel 09/14	001-700-343	52.90
SHEETZ	INV0002638	09/16/2026	Car#25 Fuel 9/15	001-700-343	67.01
7-ELEVEN	INV0002639	09/16/2026	Car#14 Fuel 09/15	001-700-343	80.00
BP	INV0002640	09/16/2026	Car#11 Fuel 09/15	001-700-343	90.91
EXXON MOBILE	INV0002641	09/17/2026	Car#27 9/16	001-700-343	63.08
7-ELEVEN	INV0002642	09/17/2026	Car#29 Fuel 09/16	001-700-343	61.18
SHEETZ	INV0002643	09/17/2026	Car#19 Fuel 9/16	001-700-343	63.00
SHEETZ	INV0002645	09/17/2026	Car#17 Fuel 09/16	001-700-343	78.00
7-ELEVEN	INV0002646	09/17/2026	Car#14 Fuel 09/16	001-700-343	66.50
SHEETZ	INV0002673	09/17/2026	Car#8 Fuel 09/16	001-700-343	40.35
PILOT	INV0002647	09/18/2026	Car#27 Fuel 09/17	001-700-343	71.31
7-ELEVEN	INV0002648	09/18/2026	Car#29 Fuel 09/17	001-700-343	35.00
SHEETZ	INV0002649	09/18/2026	Car#16 Fuel 09/17	001-700-343	94.69
7-ELEVEN	INV0002650	09/18/2026	Car#17 Fuel 09/17	001-700-343	78.00
SHEETZ	INV0002756	09/18/2026	Car#7 Fuel 09/17	001-700-343	79.05
TOWN MART CITGO	INV0002656	09/21/2026	Car#29 Fuel 9/17	001-700-343	28.49
LIBERTY GET N GO	INV0002657	09/21/2026	Car#29 Fuel 09/19	001-700-343	52.48
SHEETZ	INV0002658	09/21/2026	Car#18 Fuel 09/20	001-700-343	30.00
PILOT	INV0002659	09/21/2026	Car#21 Fuel 09/20	001-700-343	54.21
SHEETZ	INV0002660	09/21/2026	Car#21 Fuel 09/20	001-700-343	50.98
SHEETZ	INV0002661	09/21/2026	Car#10 Fuel 09/18	001-700-343	76.20
LIBERTY GET N GO	INV0002662	09/21/2026	Car#25 Fuel 09/17-	001-700-343	66.66
SHEETZ	INV0002663	09/21/2026	Car#25 Fuel 09/20	001-700-343	52.01
SHEETZ	INV0002664	09/21/2026	Car#17 Fuel 09/19	001-700-343	69.46
7-ELEVEN	INV0002665	09/21/2026	Car#14 Fuel 09/20	001-700-343	61.06
BP	INV0002666	09/21/2026	Car#3 Fuel 09/17	001-700-343	95.95
SHEETZ	INV0002667	09/21/2026	Car#26 Fuel 09/18	001-700-343	50.86
SHEETZ	INV0002668	09/21/2026	Car#15 Fuel 09/18	001-700-343	48.90
BP	INV0002669	09/21/2026	Car#11 Fuel 09/18	001-700-343	76.76
SHEETZ	INV0002674	09/21/2026	Car#8 Fuel 09/20	001-700-343	47.87
BP	INV0002675	09/21/2026	Car#8 Fuel 09/19	001-700-343	59.24

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number	Amount
PILOT	INV0002745	09/21/2026	Car#21 Fuel 09/18	001-700-343	21.76
LIBERTY GET N GO	INV0002781	09/21/2026	Fuel Can 9/18	001-700-343	22.55
SHEETZ	INV0002876	09/21/2026	Car#9 Fuel 9/18	001-700-343	64.25
SYMBOLARTS LLC	0577921	09/22/2026	CT PD Gold & Nickel Badge Pins X 50	001-700-345	320.50
DONALD B RICE TIRE CO INC	14144942	09/22/2026	Car#16 4 New Tires	001-700-343	704.00
DONALD B RICE TIRE CO INC	14145034	09/22/2026	Car#1 4 New Tires	001-700-343	704.00
CREAMERS AUTO SERVICE CEI	152491	09/22/2026	Car#25 WV Inspection & Oil Service	001-700-217	18.67
CREAMERS AUTO SERVICE CEI	152491	09/22/2026	Car#25 WV Inspection & Oil Service	001-700-343	91.82
SHEETZ	INV0002671	09/22/2026	Car#25 Fuel 9/21	001-700-343	65.51
SHEETZ	INV0002672	09/22/2026	Car#14 Fuel 09/21	001-700-343	59.75
AMAZON	INV0002878	09/22/2026	PD Flash Drives X 3 & Copy Paper	001-700-341	153.93
LIBERTY GET N GO	INV0002679	09/23/2026	Car#4 Fuel 09/21	001-700-343	85.07
SHEETZ	INV0002680	09/23/2026	Car#18 Fuel 09/22	001-700-343	70.00
TOWN MART CITGO	INV0002682	09/23/2026	Car #12 Fuel 09/20	001-700-343	84.96
SHENTEL BUSINESS	INV0002676	09/24/2026	Oct 26 CH & PD Internet Service	001-700-213	950.00
WAWA	INV0002683	09/24/2026	Car#4 Fuel 09/23	001-700-343	87.05
SHEETZ	INV0002684	09/24/2026	Car#27 Fuel 09/23	001-700-343	66.40
SHEETZ	INV0002685	09/24/2026	Car#18 Fuel 09/23	001-700-343	47.00
SHEETZ	INV0002686	09/24/2026	Car#25 Fuel 09/23	001-700-343	73.56
7-ELEVEN	INV0002687	09/24/2026	Car#14 Fuel 09/23	001-700-343	42.74
TOWN MART CITGO	INV0002688	09/24/2026	Car#12 Fuel 09/22	001-700-343	71.76
BP	INV0002689	09/24/2026	Car#7 Fuel 09/23	001-700-343	87.28
SHEETZ	INV0002692	09/25/2026	Car#17 Fuel 09/24	001-700-343	70.00
BP	INV0002693	09/25/2026	Car#11 Fuel 09-24	001-700-343	79.79
CREAMERS AUTO SERVICE CEI	152496	09/28/2026	Car#24 Headlamp Bulb &Installation	001-700-217	62.11
CREAMERS AUTO SERVICE CEI	152553	09/28/2026	152553 Car#14 Oil Serv; 4 Tires; Pads&Rotors	001-700-217	1916.92
CREAMERS AUTO SERVICE CEI	152553	09/28/2026	152553 Car#14 Oil Serv; 4 Tires; Pads&Rotors	001-700-343	367.22
CREAMERS AUTO SERVICE CEI	152555	09/28/2026	Car#6 Oil Service	001-700-343	144.31
BP	INV0002697	09/28/2026	Car#4 Fuel 09/27	001-700-343	78.11
LIBERTY GET N GO	INV0002698	09/28/2026	Car#29 Fuel 09/24	001-700-343	30.00
LIBERTY GET N GO	INV0002699	09/28/2026	Car#29 Fuel 09/26	001-700-343	65.28
SHEETZ	INV0002700	09/28/2026	Car#18 Fuel 09/27	001-700-343	38.00
SHEETZ	INV0002701	09/28/2026	Car#21 Fuel 09/27	001-700-343	51.98
MARATHON	INV0002702	09/28/2026	Car#21 Fuel 09/25	001-700-343	32.12
SHEETZ	INV0002703	09/28/2026	Car#17 Fuel 09/25	001-700-343	82.00
7-ELEVEN	INV0002704	09/28/2026	Car#14 Fuel 09/27	001-700-343	85.50
7-ELEVEN	INV0002705	09/28/2026	Car#14 Fuel 09/27	001-700-343	34.33
TOWN MART CITGO	INV0002706	09/28/2026	Car#12 Fuel 09/23	001-700-343	58.89
BP	INV0002707	09/28/2026	Car#3 09/24	001-700-343	81.24
BP	INV0002708	09/28/2026	Car#3 Fuel 09/27	001-700-343	61.51
LIBERTY GET N GO	INV0002709	09/28/2026	Car#26 Fuel 09/26	001-700-343	48.40
SHEETZ	INV0002710	09/29/2026	Car#18 Fuel 09/28	001-700-343	42.00
SHEETZ	INV0002711	09/29/2026	Car#16 Fuel 09/28	001-700-343	88.29
MARATHON	INV0002744	09/29/2026	Car#21 Fuel 09/27	001-700-343	54.56

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number	Amount
BP	INV0002755	09/29/2026	Car#7 Fuel 09/28	001-700-343	84.44
7-ELEVEN	INV0002880	09/29/2026	Car#24 Fuel 9/28	001-700-343	44.01
SHEETZ	INV0002743	09/30/2026	Car#18 Fuel 09/29	001-700-343	40.00
SHEETZ	INV0002746	09/30/2026	Car#14 Fuel 09/29	001-700-343	80.05
TOWN MART CITGO	INV0002751	09/30/2026	Car#12 Fuel 9/28	001-700-343	70.91
SHEETZ	INV0002754	09/30/2026	Car#26 Fuel 09/29	001-700-343	45.66
AMAZON	INV0002881	09/30/2026	PD Cleaning Supplies	001-700-341	4.99
SHEETZ	INV0002894	09/30/2026	Car#1 Fuel 9/29	001-700-343	96.18
				Department 700 - POLICE DEPARTMENT Total:	**33998.96**
Department: 704 - POLICE-SPECIAL DUTY					
GALLS, LLC	036049716	09/14/2026	Xng Guards Rain JacketsX2 & Safety Vest	001-704-345	101.22
				Department 704 - POLICE-SPECIAL DUTY Total:	**101.22**
Department: 750 - STREETS & HIGHWAYS					
COMCAST CORPORATION	INV0002330	09/02/2026	Sept 26 MD Internet Service	001-750-213	105.81
LIBERTY GET N GO	INV0002785	09/02/2026	P23 Fuel 08/31	001-750-343	117.27
TOWN MART CITGO	INV0002802	09/02/2026	P12 Fuel 8/31	001-750-343	85.55
LIBERTY GET N GO	INV0002812	09/02/2026	D23 Fuel 8/31	001-750-343	177.08
MID ATLANTIC ENTRY MD LLC	41005	09/03/2026	MD Gate Repairs	001-750-215	1919.25
GENUINE PARTS COMPANY - N	980150	09/03/2026	Hydraulic Hose for Bobcat	001-750-216	15.72
TOWN MART CITGO	INV0002778	09/03/2026	M19 Fuel 9/1	001-750-343	40.13
7-ELEVEN	INV0002813	09/03/2026	P16 Fuel 9/03	001-750-343	99.09
WALMART INC	INV0002803	09/04/2026	9/03 MD Coffee	001-750-341	26.94
LIBERTY GET N GO	INV0002804	09/07/2026	Can Fuel 9/3	001-750-343	9.14
TOWN MART CITGO	INV0002805	09/07/2026	P12 Fuel 9/4	001-750-343	73.27
LIBERTY GET N GO	INV0002814	09/07/2026	Sweeper Fuel 9/4	001-750-343	112.04
CHARLES TOWN UTILITY BOAF	INV0002476	09/10/2026	Aug 26 MD Water Service	001-750-213	117.79
LIBERTY GET N GO	INV0002779	09/10/2026	S590 Fuel 09/08	001-750-343	89.76
LIBERTY GET N GO	INV0002780	09/10/2026	Fuel Can 9/8	001-750-343	20.36
LIBERTY GET N GO	INV0002815	09/10/2026	P16 Fuel 9/8	001-750-343	113.04
ENVIRO-TECH PEST SERVICES	496642	09/11/2026	Sept 26 CWHall Pest Service	001-750-215	125.19
ENVIRO-TECH PEST SERVICES	496646	09/11/2026	Sept 26 RH Pest Service	001-750-215	79.18
TOWN MART CITGO	INV0002806	09/11/2026	P12 Fuel 9/9	001-750-343	100.19
HOME DEPOT INC	INV0002816	09/11/2026	Rouss Hall Handle Replacement	001-750-215	40.57
GENUINE PARTS COMPANY - N	981733	09/14/2026	CH22 Oil & Filter	001-750-343	49.11
LIBERTY GET N GO	INV0002788	09/14/2026	P23 Fuel 9/10	001-750-343	115.63
HOME DEPOT INC	INV0002817	09/14/2026	City Hall Keys X 5	001-750-341	29.85
GENUINE PARTS COMPANY - N	981867	09/15/2026	Head Light Glass Cleaner	001-750-216	14.02
TRACTOR SUPPLY	INV0002789	09/15/2026	S26 Bolts	001-750-216	4.98
AMAZON	INV0002790	09/15/2026	CH Air Filters	001-750-341	89.99
SAVE-A-LOT	INV0002807	09/15/2026	MD Water X 2	001-750-341	18.98
TIREVILLE	18127	09/16/2026	CH 22 Tires X 4	001-750-343	1128.88
GENUINE PARTS COMPANY - N	981896	09/16/2026	5 Gal Paint Thinner	001-750-341	59.86
LIBERTY GET N GO	INV0002818	09/16/2026	Sweeper Fuel 9/14	001-750-343	68.02

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number		Amount
APPLE VALLEY WASTE SERVICI	0007147561	09/17/2026	Aug 26 MD Trash Service	001-750-230		695.51
7-ELEVEN	INV0002644	09/17/2026	BI Jeep Fuel 09/16	001-750-343		70.72
HOME DEPOT INC	INV0002792	09/17/2026	CH Air Filters	001-750-341		56.91
SUNOCO	INV0002820	09/17/2026	P16 Fuel 118.23	001-750-343		118.23
TOWN MART CITGO	INV0002808	09/21/2026	P12 Fuel 9/18	001-750-343		80.06
ADVANCED AUTO PARTS PROI	INV0002819	09/22/2026	Sweeper Exhaust Fluid	001-750-216		49.20
WAWA	INV0002681	09/23/2026	BI Fuel 9/22	001-750-343		57.10
LIBERTY GET N GO	INV0002782	09/23/2026	M19 Fuel 9/21	001-750-343		49.81
LIBERTY GET N GO	INV0002821	09/23/2026	Sweeper Fuel 9/21	001-750-343		112.95
LIBERTY GET N GO	INV0002783	09/24/2026	Fuel Can 9/22	001-750-343		8.72
HOME DEPOT INC	INV0002784	09/24/2026	Concrete for Liberty St 4-Way Stop Signs	001-750-341		25.88
LIBERTY GET N GO	INV0002793	09/25/2026	P23 Fuel 9/23	001-750-343		128.72
LIBERTY GET N GO	INV0002822	09/25/2026	P16 Fuel 9/23	001-750-343		102.88
LIBERTY GET N GO	INV0002809	09/28/2026	Can Fuel 9/24	001-750-343		8.72
LIBERTY GET N GO	INV0002823	09/28/2026	B12 Fuel 9/24	001-750-343		217.93
WASTE MANAGEMENT INC	3476564-2413-7	09/29/2026	Oct 26 MD Waste Service	001-750-230		334.93
SHEETZ	INV0002824	09/29/2026	P25 Fuel 9/28	001-750-343		127.81
SHEETZ	INV0002777	09/30/2026	CE Trax Fuel 9/29	001-750-343		49.43
LIBERTY GET N GO	INV0002810	09/30/2026	P12 Fuel 9/28	001-750-343		70.04
7-ELEVEN	INV0002825	09/30/2026	P16 Fuel 9/28	001-750-343		123.03
					Department 750 - STREETS & HIGHWAYS Total:	**7535.27**
Department: 900 - PARKS & REC						
TRIVAGO	INV0002494	09/04/2026	Hotel for NRPA Conf 09/26-28	001-900-214		615.00
					Department 900 - PARKS & REC Total:	**615.00**
Department: 903 - FAIR ASSOC/FESTIVAL						
WALMART INC	INV0002794	09/02/2026	Car Show 26 Snacks & Drinks & Index Card	001-903-341		138.02
ORTEGA'S TACO SHOP	INV0002795	09/07/2026	Car Show 26 Volunteer Lunch X 2	001-903-341		26.74
AC &T CO., INC	59784	09/16/2026	26 Car Show PT Service	001-903-230		1046.00
					Department 903 - FAIR ASSOC/FESTIVAL Total:	**1210.76**
					Fund 001 - GENERAL FUND Total:	**52460.87**
Fund: 207 - PARKS & REC						
Department: 900 - PARKS & REC						
HOME DEPOT INC	INV0002786	09/03/2026	Light Fixtures Evitts Run Bathroom	207-900-341		74.97
HOME DEPOT INC	INV0002787	09/07/2026	Light Fixtures JMP Veterans Memorial	207-900-341		137.94
CHARLES TOWN UTILITY BOAF	INV0002476	09/10/2026	Aug 26 Water Service EV Run Park Bathroom	207-900-213		56.16
CHARLES TOWN UTILITY BOAF	INV0002476	09/10/2026	Aug 26 Water Service JMP Pool	207-900-213		829.88
APPLE VALLEY WASTE SERVICI	0007147561	09/17/2026	Aug 26 JMP Trash Service	207-900-230		553.14
JEFFERSON PUBLISHING COMI	74717	09/17/2026	RFP Clean Parks Green Infrastructure Master I	207-900-220		24.06
HOME DEPOT INC	INV0002791	09/17/2026	Paper Lawn Bags	207-900-341		11.25
340 CAR WASH	INV0002677	09/21/2026	P&R Jeep Detailing	207-900-217		13.00
SHEETZ	INV0002678	09/23/2026	P&R Jeep Fuel 09/22	207-900-343		54.75
AC &T CO., INC	55890R	09/24/2026	Sept 26 Willingham Knolls PT Service	207-900-230		115.00

Vendor Name	Payable Numbe	Post Date	Description (Item)	Account Number		Amount
AC &T CO., INC	55891R	09/24/2026	Sept 26 Skate Park PT Service	207-900-230		178.00
JEFFERSON PUBLISHING COMI	74784	09/24/2026	9/3 RFP Clean Park Intiative	207-900-220		25.90
JEFFERSON PUBLISHING COMI	747856	09/24/2026	9/10 RFP Clean Parks Initiative	207-900-220		25.90
SOUTHERN STATES INC	W565982	09/24/2026	Grass Seed for Happy Retreat	207-900-341		89.99
JEFFERSON PUBLISHING COMI	74797	09/28/2026	9/17 Parks Manager Job Posting	207-900-220		83.40
AC &T CO., INC	10072EU	09/29/2026	Sept 26 JMP PT Service	207-900-230		115.00
COMCAST CORPORATION	INV0002694	09/29/2026	Sept 26 JMP Pool Internet Service	207-900-213		183.81
					Department 900 - PARKS & REC Total:	**2572.15**
					Fund 207 - PARKS & REC Total:	**2572.15**
					Grand Total:	**55033.02**

Report Summary

Fund Summary

Fund	Payment Amount
001 - GENERAL FUND	52460.87
207 - PARKS & REC	2572.15
Grand Total:	**55033.02**

Account Summary

Account	Account Name	Payment Amount
001-114-020	DUE FROM WATER DEPT	87.00
001-402-214	ECO DEV - TRAVEL	157.31
001-402-222	ECONOMIC DEV - DUES & SUBSCRIP	51.34
001-402-341	ECONOMIC DEV - DEPT. SUPPLIES	9.63
001-410-221	CITY CO Training & Education	28.00
001-413-220	TREAS Advertising/Legal Publ	164.90
001-417-222	ATTORNEY DUES & SUBSCRIPTIONS	899.19
001-417-341	DEPARTMENT SUPPLIES	15.50
001-425-214	ENFORCEMENT AG -	210.75
001-425-341	ENFORCEMENT AG - DEPT. SUPPLIE	169.99
001-436-211	BI Telephone	40.04
001-436-214	BI Travel Expense	225.90
001-436-223	BI PROFESSIONAL SERVICES	2000.00
001-437-214	P&Z Travel Expense	654.90
001-437-220	P&Z Advertising/Legal Publ	107.14
001-437-222	P&Z Dues & Subscriptions	105.99
001-440-213	CH Utilities	1376.54
001-440-218	CH Postage	499.43
001-440-219	CH Buildings & Equipment Rents	505.23
001-440-222	CH Dues & Subscriptions	181.43
001-440-230	CH Contracted Services	1135.54
001-440-341	CH Departmental Supplies	291.23
001-571-341	PARKING Departmental Supplies	82.68
001-700-213	PD UTILITIES	1126.65
001-700-217	PD R&M AUTO	3028.24
001-700-220	PD ADVERTISING & LEGAL PUBLICA	6.26
001-700-222	PD DUES AND SUBSCRIPTIONS	110.00
001-700-230	PD CONTRACTED SERVICES	1024.99
001-700-341	PD DEPARTMENTAL SUPPLIES	2087.60
001-700-343	PD AUTO SUPPLIES (GAS OIL TIRE	11339.72
001-700-345	PD UNIFORMS	3530.50
001-700-353	PD COMPUTER SOFTWARE/TECH	11745.00
001-704-345	POL SPEC DUTY UNIFORMS	101.22
001-750-213	STREETS UTILITIES	223.60

Account Summary

Account	Account Name	Payment Amount
001-750-215	STREETS R&M BLDG AND GROUNDS	2164.19
001-750-216	STREETS R&M EQUIPMENT	83.92
001-750-230	STREETS CONTRACTED SERVICES	1030.44
001-750-341	STREETS DEPARTMENT SUPPLIES	308.41
001-750-343	STREETS AUTO SUPPLIES GAS OIL	3724.71
001-900-214	P&R TRAVEL	615.00
001-903-230	FAIR/FESTIVAL Contracted Svcs	1046.00
001-903-341	FAIR/FESTIVAL Department Suppy	164.76
207-900-213	UTILITIES	1069.85
207-900-217	P&R REPAIR & MAINTENANCE AUTO	13.00
207-900-220	ADVERTISING/LEGAL PUBLICATIONS	159.26
207-900-230	CONTRACTED SERVICES	961.14
207-900-341	DEPARTMENTAL SUPPLIES	314.15
207-900-343	P&R AUTO SUPPLIES (GAS, OIL & TIRES)	54.75
	Grand Total:	**55033.02**

Project Account Summary

Project Account I		Payment Amount
None		55033.02
	Grand Total:	**55033.02**

Authorization Signatures

. COUNCIL MEMBER

. COUNCIL MEMBER

Expense Approval Report

Charles Town, WV

By Fund

Post Dates 10/6/2026 - 10/16/2026

Vendor Name	Payable Number	Post Date	Description (Item)	Account Number		Amount
Fund: 001 - GENERAL FUND						
WV PERS (CPRB)	INV0002868	10/07/2026	July MPFRS	001-224-000		18425.38
WV PERS (CPRB)	INV0002869	10/07/2026	Aug 26 MPFRS	001-224-000		11278.34
WV STATE TREASURER'S OFFI	INV0002842	10/08/2026	Sept 26 Municipal Court Fees	001-201-050		3361.43
PEIA	INV0002856	10/13/2026	Sept 26 Employee PEIA Insurance Contribution	001-225-000		5189.82
PEIA	INV0002857	10/13/2026	Sept 26 Employee RHBT Contribution	001-225-000		247.80
US BANK	INV0002916	10/13/2026	Sept 26 AP PCard Payment	001-201-110		36546.35
US BANK	INV0002917	10/13/2026	Sept 26 CH & PD PCard Payment	001-201-110		8889.03
US BANK	INV0002918	10/13/2026	Sept 26 Fleet PCard Payment	001-201-110		8105.88
UNITED WAY OF THE EASTERN	INV0002970	10/15/2026	Sept 26 Teen Court Fees	001-201-070		300.00
SUN LIFE	INV0002990	10/16/2026	Nov 26 Employee Dental Insurance Contributio	001-225-010		228.28
						92572.31
Department: 402 - ECONOMIC DEVELOPMENT						
PEIA	INV0002856	10/13/2026	Sept 26 ED PEIA Insurance Contribution	001-402-105		687.08
PEIA	INV0002857	10/13/2026	Sept 26 ED RHBT Contribution	001-402-111		50.15
SUN LIFE	INV0002990	10/16/2026	Nov 26 ED Dental Insurance Contribution	001-402-105		94.91
					Department 402 - ECONOMIC DEVELOPMENT Total:	**832.14**
Department: 412 - CITY MANAGER'S OFFICE						
PEIA	INV0002856	10/13/2026	Sept 26 CMO PEIA Insurance Contribution	001-412-105		1.98
SUN LIFE	INV0002990	10/16/2026	Nov 26 CMO Dental Insurance Contribution	001-412-105		-354.76
					Department 412 - CITY MANAGER'S OFFICE Total:	**-352.78**
Department: 413 - TREASURER'S OFFICE						
PEIA	INV0002856	10/13/2026	Sept 26 TR PEIA Insurance Contribution	001-413-105		1376.14
PEIA	INV0002857	10/13/2026	Sept 26 TR RHBT Contribution	001-413-111		100.30
HDL COMPANIES INC	09302026	10/15/2026	Sept 26 B&O Collections Service	001-413-230		7046.94
SUN LIFE	INV0002990	10/16/2026	Nov 26 TR Dental Insurance Contribution	001-413-105		261.94
					Department 413 - TREASURER'S OFFICE Total:	**8785.32**
Department: 415 - CITY CLERK'S OFFICE						
PEIA	INV0002856	10/13/2026	Sept 26 CK PEIA Insurance Contribution	001-415-105		1523.48
PEIA	INV0002857	10/13/2026	Sept 26 CK RHBT Contribution	001-415-111		50.15
SUN LIFE	INV0002990	10/16/2026	Nov 26 CK Dental Insurance Contribution	001-415-105		124.86
					Department 415 - CITY CLERK'S OFFICE Total:	**1698.49**
Department: 416 - POLICE JUDGE'S OFFICE						
Robert Dallmann	INV0002952	10/15/2026	Fuel Reimbursement for Subpoena Case	001-416-223		76.76
					Department 416 - POLICE JUDGE'S OFFICE Total:	**76.76**

Vendor Name	Payable Number	Post Date	Description (Item)	Account Number		Amount
Department: 417 - CITY ATTORNEY						
PEIA	INV0002856	10/13/2026	Sept 26 CA PEIA Insurance Contribution	001-417-105		1.98
BOWLES RICE LLP	1265218	10/15/2026	TIF District Attorney Services Thru 10/01	001-417-223		709.50
SUN LIFE	INV0002990	10/16/2026	Nov 26 CA Dental Insurance Contribution	001-417-105		122.73
					Department 417 - CITY ATTORNEY Total:	**834.21**
Department: 425 - ENFORCEMENT AGENCY						
PEIA	INV0002856	10/13/2026	Sept 26 CE PEIA Insurance Contribution	001-425-105		687.08
PEIA	INV0002857	10/13/2026	Sept 26 CE RHBT Contribution	001-425-111		50.15
SOUTH CENTRAL PLANNING &	27T-491	10/15/2026	Sept 26 Permit Software	001-425-230		250.00
SUN LIFE	INV0002990	10/16/2026	Nov 26 CE Dental Insurance Contribution	001-425-105		81.66
					Department 425 - ENFORCEMENT AGENCY Total:	**1068.89**
Department: 436 - BUILDING INSPECTION						
PEIA	INV0002856	10/13/2026	Sept 26 BI PEIA Insurance Contribution	001-436-105		1.98
SUN LIFE	INV0002990	10/16/2026	Nov 26 BI Dental Insurance Contribution	001-436-105		141.00
					Department 436 - BUILDING INSPECTION Total:	**142.98**
Department: 437 - PLANNING & ZONING						
PEIA	INV0002856	10/13/2026	Sept 26 PZ PEIA Insurance Contribution	001-437-105		4421.12
PEIA	INV0002857	10/13/2026	Sept 26 PZ RHBT Contribution	001-437-111		200.60
SOUTH CENTRAL PLANNING &	27T-491	10/15/2026	Sept 26 Permit Software	001-437-353		730.00
KIMLEY-HORN AND ASSOCIAT	37325832	10/16/2026	Sept 26 Planning & Site Review	001-437-230		1596.72
SUN LIFE	INV0002990	10/16/2026	Nov 26 PZ Dental Insurance Contribution	001-437-105		475.53
					Department 437 - PLANNING & ZONING Total:	**7423.97**
Department: 440 - CITY HALL						
HIRE LEVEL HCM INC	0000178829	10/09/2026	10/09/2026 GF PAYROLL SERVICES	001-440-230		296.52
POTOMAC EDISON COMPANY	INV0002895	10/09/2026	Sept 26 Visitor Center Electricity Service	001-440-213		1395.07
POTOMAC EDISON COMPANY	INV0002899	10/09/2026	Sept 26 RH 2nd Floor	001-440-213		279.03
POTOMAC EDISON COMPANY	INV0002900	10/09/2026	Sept 26 CWHall Electricity	001-440-213		1580.76
PEIA	INV0002856	10/13/2026	Sept 26 CH PEIA Insurance Contribution	001-440-105		56.98
TEK ADVISORS	4109	10/15/2026	Sept 26 Tech Service	001-440-230		11162.72
JOHNSON CONTROLS US HOLI	42857197	10/15/2026	FY27 2Qrtr CWHall Alarm Service	001-440-230		414.60
SUSTAINABLE STRATEGIES DC	5203	10/15/2026	Sept 26 Grant Retainer	001-440-230		5000.00
KONICA MINOLTA BUSINESS S	820100305	10/15/2026	Oct 26 CH Monthly Webex Service	001-440-211		444.58
MILLENIUM INSURANCE GROI	COC 11.2026	10/15/2026	November 26 Insurance Broker Retainer	001-440-223		1800.00
FRONTIER COMMUNICATIONS	INV0002955	10/15/2026	Oct 26 RH Elevator Alarm	001-440-211		90.49
FRONTIER COMMUNICATIONS	INV0002956	10/15/2026	Oct 26 CWHall Alarm #1 Service	001-440-211		97.37
PITNEY BOWES BANK INC PUR	INV0002965	10/15/2026	Sept 26 Postage Refill	001-440-218		200.00
FRONTIER COMMUNICATIONS	INV0002988	10/16/2026	Oct 26 RH Fire Alarm #1 & 2	001-440-211		252.17
SUN LIFE	INV0002990	10/16/2026	Nov 26 CH Dental Insurance Contribution	001-440-105		162.30
					Department 440 - CITY HALL Total:	**23232.59**
Department: 444 - CONT/TRNSFR 2 OTHR FUNDS						
Ron Widmyer	INV0002966	10/15/2026	Revive Grant Reimbursement113 W Washingtc	001-444-568		10000.00
					Department 444 - CONT/TRNSFR 2 OTHR FUNDS Total:	**10000.00**

Vendor Name	Payable Number	Post Date	Description (Item)	Account Number		Amount
Department: 571 - PARKING						
PEIA	INV0002856	10/13/2026	Sept 26 PK PEIA Insurance Contribution	001-571-105		687.08
PEIA	INV0002857	10/13/2026	Sept 26 PK RHBT Contribution	001-571-111		50.15
SUN LIFE	INV0002990	10/16/2026	Nov 26 PK Dental Insurance Contribution	001-571-105		65.97
					Department 571 - PARKING Total:	**803.20**
Department: 700 - POLICE DEPARTMENT						
WV PERS (CPRB)	64023	10/07/2026	May 2026 Late Fee	001-700-106		50.00
PEIA	INV0002856	10/13/2026	Sept 26 PD PEIA Insurance Contribution	001-700-105		14868.70
PEIA	INV0002857	10/13/2026	Sept 26 PD RHBT Contribution	001-700-111		752.25
JEFFERSON COUNTY EMERGEI	667	10/15/2026	June26 CAD/Mobile Data & Cradlepoint Device	001-700-213		614.43
JEFFERSON COUNTY EMERGEI	670	10/15/2026	July 26 CAD/Mobile Data & Cradlepoint Device:	001-700-213		591.82
Daigle Law Group LLC	7228	10/15/2026	PD Policy Development	001-700-223		2350.00
KONICA MINOLTA BUSINESS S	820100305	10/15/2026	Oct 26 PD Monthly Webex Service	001-700-211		509.47
FIDELITY POWER SYSTEMS	FPSMC0076934	10/15/2026	661 S George Generator Contract 3rd Instalmer	001-700-216		3930.00
COMCAST CORPORATION	INV0002950	10/15/2026	Oct 26 PD TV Subscription	001-700-213		10.45
DOCTOR ROBERT JONES	INV0002953	10/15/2026	Nathan Daniel Physical	001-700-223		175.00
WITMER PUBLIC SAFETY GROI	INV974441	10/15/2026	Baton Holder X 2	001-700-345		86.00
SUN LIFE	INV0002990	10/16/2026	Nov 26 PD Dental Insurance Contribution	001-700-105		1875.17
					Department 700 - POLICE DEPARTMENT Total:	**25813.29**
Department: 750 - STREETS & HIGHWAYS						
PEIA	INV0002856	10/13/2026	Sept 26 MD PEIA Insurance Contribution	001-750-105		3515.62
PEIA	INV0002857	10/13/2026	Sept 26 MD RHBT Contribution	001-750-111		150.45
LYLE C TABB & SONS, INC.	2026 9 171	10/15/2026	Sept 26 Box Rental	001-750-230		900.00
Ware Hauling LLC	2782	10/15/2026	Shale to Fill Holes at MD	001-750-215		208.03
SUN LIFE	INV0002990	10/16/2026	Nov 26 MD Dental Insurance Contribution	001-750-105		362.55
					Department 750 - STREETS & HIGHWAYS Total:	**5136.65**
Department: 751 - STREET LIGHT UTILITIES						
POTOMAC EDISON COMPANY	INV0002811	10/06/2026	Sept 26 Crosswinds Electricty	001-751-213		183.06
POTOMAC EDISON COMPANY	INV0002896	10/09/2026	Sept 26 Electricity Depot District #2	001-751-213		17.31
POTOMAC EDISON COMPANY	INV0002897	10/09/2026	Sept 26 Electricity Depot District #1	001-751-213		13.82
POTOMAC EDISON COMPANY	INV0002898	10/09/2026	Sept 26 Electricity Depot District #3	001-751-213		11.02
					Department 751 - STREET LIGHT UTILITIES Total:	**225.21**
Department: 900 - PARKS & REC						
SUN LIFE	INV0002990	10/16/2026	Nov 26 P&R Dental Insurance Contribution	001-900-105		-90.78
					Department 900 - PARKS & REC Total:	**-90.78**
Department: 901 - VISITORS CENTER						
JEFFERSON COUNTY CONVEN	INV0002958	10/15/2026	Sept 26 Hotel/Motel Tax Revenue	001-901-567		7665.65
					Department 901 - VISITORS CENTER Total:	**7665.65**
					Fund 001 - GENERAL FUND Total:	**185868.10**
					Grand Total:	**185868.10**

Report Summary

Fund Summary

Fund	Payment Amount
001 - GENERAL FUND	185868.1
Grand Total:	**185868.1**

Account Summary

Account	Account Name	Payment Amount
001-201-050	State Court Fees Payable	3361.43
001-201-070	TEEN COURT FEES PAYABLE	300.00
001-201-110	PCARD PAYABLE	53541.26
001-224-000	Retirement Contributions Payab	29703.72
001-225-000	Insurance Contributions Payabl	5437.62
001-225-010	Dental & Vision Payable	228.28
001-402-105	ECONOMIC DEV - GROUP INSURANCE	781.99
001-402-111	ECONOMIC DEV - OPEB	50.15
001-412-105	CMO Group Insurance	-352.78
001-413-105	TREAS Group Insurance	1638.08
001-413-111	TREAS OPEB Other	100.30
001-413-230	TREAS Contracted Services	7046.94
001-415-105	CLERK Group Insurance	1648.34
001-415-111	CLERK OPEB	50.15
001-416-223	PJO Professional Services	76.76
001-417-105	ATTORNEY INSURANCE	124.71
001-417-223	ATTORNEY Professional Services	709.50
001-425-105	ENFORCEMENT AG - GROUP INSURAN	768.74
001-425-111	ENFORCEMENT AG - OPEB	50.15
001-425-230	EA Contracted Services	250.00
001-436-105	BI Group Insurance	142.98
001-437-105	P&Z Group Insurance	4896.65
001-437-111	P&Z OPEB	200.60
001-437-230	P&Z Contracted Services	1596.72
001-437-353	P&Z COMPUTER SOFTWARE	730.00
001-440-105	CH Group Insurance	219.28
001-440-211	CH Telephone	884.61
001-440-213	CH Utilities	3254.86
001-440-218	CH Postage	200.00
001-440-223	CH Professional Services	1800.00
001-440-230	CH Contracted Services	16873.84
001-444-568	COMMUNITY CONTRIBUTIONS/TRANSFERS	10000.00
001-571-105	PARKING Group Insurance	753.05
001-571-111	PARKING OPEB	50.15
001-700-105	PD GROUP INSURANCE	16743.87

Account Summary

Account	Account Name	Payment Amount
001-700-106	PD RETIREMENT EXPENSE	50.00
001-700-111	PD OPEB	752.25
001-700-211	PD TELEPHONE	509.47
001-700-213	PD UTILITIES	1216.70
001-700-216	PD R&M EQUIPMENT	3930.00
001-700-223	PD PROFESSIONAL SERVICES	2525.00
001-700-345	PD UNIFORMS	86.00
001-750-105	STREETS GROUP INSURANCE	3878.17
001-750-111	STREETS OPEB	150.45
001-750-215	STREETS R&M BLDG AND GROUNDS	208.03
001-750-230	STREETS CONTRACTED SERVICES	900.00
001-751-213	STREET LIGHT UTILITIES	225.21
001-900-105	P&R Group Insurance	-90.78
001-901-567	VISITOR CTR CONTRIBUTIONS	7665.65
	Grand Total:	**185868.10**

Project Account Summary

Project Account Ke	Payment Amount
None	185868.10
Grand Total:	**185868.10**

Authorization Signatures

. COUNCIL MEMBER

. COUNCIL MEMBER

Expense Approval Report

Charles Town, WV

By Fund

Payment Dates 10/16/2026 - 10/16/2026

Vendor Name	Payable Number	Post Date	Description (Item)	Account Number	Amount
Fund: 200 - CAPITAL RESERVE					
Department: 975 - GENERAL GOVERNMENT					
TYLER TECHNOLOGIES, INC	025-569053	10/16/2026	Tyler 10 Migration My Civic App Configuration	200-975-459	8555.00
				Department 975 - GENERAL GOVERNMENT Total:	**8555.00**
				Fund 200 - CAPITAL RESERVE Total:	**8555.00**
				Grand Total:	**8555.00**

Report Summary

Fund Summary

Fund	Payment Amount
200 - CAPITAL RESERVE	8555.00
Grand Total:	**8555.00**

Account Summary

Accou	Account Name	Payment Amount
200-975-459	Gen Gov Capital Outlay-Technol	8555.00
	Grand Total:	**8555.00**

Project Account Summary

Project Account	Payment Amount
None	8555.00
Grand Total:	**8555.00**

Authorization Signatures

. COUNCIL MEMBER

. COUNCIL MEMBER

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Ordinance
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2061: An Ordinance to Approve the July 2026 Replacement Pages to the Codified Ordinance

ATTACHMENTS:

- Ordinance to Approve the July 2026 Replacement Pages - signed.pdf

CITY OF CHARLES TOWN

AN ORDINANCE TO APPROVE THE JULY 2026 REPLACEMENT PAGES TO THE CODIFIED ORDINANCES.

WHEREAS, certain provisions within the Codified Ordinances should be amended to conform with current State law; and

WHEREAS, various ordinances of a general and permanent nature have been passed by Council which should be included in the Codified Ordinances; and

WHEREAS, Council has heretofore entered into a contract with the Walter H. Drane Company to prepare and publish such revision; and

WHEREAS, the codification of such ordinances, together with the new matter to be adopted, the matters to be amended and those to be repealed are before the Council;

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF CHARLES TOWN, WEST VIRGINIA:

Section 1. That the ordinances of the City of Charles Town, West Virginia, of a general and permanent nature, as revised, recodified, rearranged and consolidated into component codes, chapters, articles and sections within the July 2026 Replacement Pages to the Codified Ordinances are hereby approved and adopted.

Section 2. That the following sections and articles are hereby added, amended or repealed as respectively indicated in order to comply with current State law:

Part Three - Traffic Code

333.01	Driving Under the Influence. (Amended)

Part Five - General Offenses Code

545.02	Carrying A Deadly Weapon Without Provisional License or Other Authorization by Persons Under Twenty-One Years of Age. (Repealed)
545.03	Exemptions From Licensing Fees. (Amended)
545.04	Persons Prohibited from Possession of Firearms. (Amended)
545.05	Possession of Deadly Weapons by Minors Prohibited. (Amended)

Section 3. This Ordinance shall become effective from the date of its adoption.

CITY OF CHARLES TOWN

Mayor

Attest:

Deputy City Clerk

Approved and enacted this 5th day of October, 2026.

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Information Only
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2062: Oath of Office - Thomas Mitchell Board of Parks and Recreation Commission

ATTACHMENTS:
- Thomas Mitchell Oath - 10-7-26.pdf

CITY OF CHARLES TOWN, WEST VIRGINIA
BOARD OF PARKS AND RECREATION COMMISSION
OATH OF OFFICE

I, **THOMAS MITCHELL,** do solemnly swear that I will support the Constitution of the United States, the Constitution of the State of West Virginia, and the laws of the City of Charles Town.

I, **THOMAS MITCHELL,** do solemnly swear that I will faithfully discharge and perform the duties of the position of Commissioner for the City of Charles Town Board of Parks and Recreation Commission to the best of my skill, ability, and judgment according to law.

Thomas Mitchell

The above oath was taken and subscribed before the Mayor of Charles Town, on this 7th day of October 2026.

Micheal George
Mayor

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Report
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2063: Infrastructure Committee Report - October 1, 2026

ATTACHMENTS:

- Report_ Infrastructure October 1, 2026.pdf

City of Charles Town

Infrastructure Committee

Report from October 1, 2026

Meeting Link: https://charlestownwv.granicus.com/player/clip/2178?view_id=1&redirect=true

I. CALL TO ORDER: Thursday, October 1, 2026 at 5:00 PM - City Hall

Councilmembers Present: Elizabeth Ricketts, Alden Roth, Jim Kratovil
Staff Present: Cory Lewis, James Newman
Guests: Zach Judy from Greenway Engineering

II. UNFINISHED BUSINESS

2026-1924: Stormwater Issues and Updates

The Committee reviewed stormwater issues, hydrological and hydraulic data, and details of the stormwater study on the old town's 10 distinct watersheds with staff from Greenway Engineering. The committee discussed the possibility of exploring zoning or ordinances to protect karst areas, requiring more stormwater assessment of in-fill projects, ability of City to contract with engineering firm for on-call services, and how best to move forwards with assessing and addressing stormwater concerns.

Recommendation to Council: *The Committee recommends moving forward with all needed next phases to bring shovel ready solutions to Watershed 3 and then to continue to assess the study and recommend either full watersheds or specifically identified issues for further analysis.*

2026-1935: Expansion of Walkability Grant - Referral from City Council

The Committee discussed the current grant parameters and heard feedback from staff on potential improvements to the program and design guidelines. The Committee would like to continue assessing other municipal sidewalk programs and look for opportunities to overhaul the program to more effectively leverage funding for sidewalks. The Committee discussed with staff the immediately needed improvements for effectiveness with the grant program.

Recommendation to Council: *Continue to assess opportunities for revamping the grant program, but in the meantime,*

- ***i****. Increase the amount for each award for inflation to $7,000*
- ***ii.*** *Add design detail for brick sidewalks into the standards which will require a concrete base and proper curbs.*
- ***iii****. Allow corner lots with two sidewalk sections to apply for a double award.*
- ***iv****. Remove language in the grant prohibiting brick where it does not already exist.*

III. NEW BUSINESS

NONE.

IV. ADJOURNMENT

Adjourned: 6:45PM
Next meeting: Monday, October 26th at 4:30PM

City Council
101 East Washington Street
Charles Town, WV 25414

Meeting: 10/19/26
Department: City Council
Category: Resolution
Initiator:

SCHEDULED

AGENDA ITEM (ID #)

2026-2064: 2026-008 Resolution on Transmission Line Projects

ATTACHMENTS:

- 2026-008 - Resolution on Transmission Line Projects.pdf

City of Charles Town
101 East Washington Street, P.O. Box 14, Charles Town, WV 25414
Phone: (304) 725-2311 ♦ Web: www.charlestownwv.us

RESOLUTION

RESOLUTION WHEREAS, the 500 kV Mid-Atlantic Link (MARL) project and the proposed 765 kV Valley Link North project and 500 kV Gore-Doubs-Goose Creek project will greatly expand the current transmission line corridor and expand its high-voltage footprint through multiple counties in West Virginia, including Jefferson County and its municipalities; and

WHEREAS, the MARL, Valley Link North, and Gore-Doubs-Goose Creek projects intended to transport electricity across West Virginia to serve increased energy demands and power Virginia's economic development while it alternatively creates and leaves a destructive path through Charles Town; and

WHEREAS, the proposed route could take a more direct path to Loudoun County, instead it proposes to divert through Jefferson County for the sole purpose of paralleling existing transmission lines inevitably leaving an expanded path of destruction with significant and irreparable harm to our historic community, undermine the City's economic development strides, and deter visitors and tourism-based initiatives; and

WHEREAS, the MARL project ultimately serves no purpose to Charles Town or its consumers, but instead, our citizens will naturally absorb a significant portion of the combined upgrade costs through regional rate increases ultimately creating undue and increased hardship for residents with already rising electric costs.

NOW, THEREFORE WE, the members Of the Charles Town City Council, do hereby adamantly oppose the siting or construction of the MARL 500kV or 765 kV Valley Link or 500 kV Gore-Doubs Goose Creek overhead transmission lines within Jefferson County or the municipal boundaries of the City of Charles Town, as such facilities would damage natural beauty, diminish property values, impair tourism and confer no commensurate benefit on the local community while disrupting the lives of families in the path of construction and forcing our residents to pay for northern Virginia energy demands through higher consumer electricity rates; and

BE IT FURTHER RESOLVED that we call on all elected officials representing Jefferson County to join the City of Charles Town in opposing this project in addition to directing this Resolution be provided to PJM Interconnection, the corporate entities proposing MARL, Valley Link North, and Goore-Doubs-Goose Creek projects, the West Virginia Public Service Commission, the Virginia State Corporation Commission and to state and federal elected officials so they may be fully informed of the City's position and concerns. Adopted this 5th day of October 2026 by vote of the Charles Town City Council.

Micheal George
Mayor

Attest:
Carolyn Vezzosi
Carolyn Vezzosi
Deputy City Clerk