ORIGINAL

CONTRACT RESULTING FROM REQUEST FOR PROPOSAL NUMBER 10090080-E, Body Worn Camera (BWC) System

This Contract (Contract) is entered into by and between the City of San Diego, a municipal corporation (City), and the successful proposer to Request for Proposal (RFP) # 10090080-E, Body Worn Camera (BWC) System (Contractor).

RECITALS

On or about 7/28/2023, City issued an RFP to prospective proposers on services to be provided to the City. The RFP and any addenda and exhibits thereto are collectively referred to as the "RFP." The RFP is attached hereto as Exhibit A.

City has determined that Contractor has the expertise, experience, and personnel necessary to provide the services.

City wishes to retain Contractor to provide a user-friendly, cloud-based Body Worn Camera (BWC) system as further described in the Scope of Work, attached hereto as Exhibit B. (Services).

For good and valuable consideration, the sufficiency of which is acknowledged, City and Contractor agree as follows:

ARTICLE I
CONTRACTOR SERVICES

1.1 Scope of Work. Contractor shall provide the Services to City as described in Exhibit B which is incorporated herein by reference. Contractor will submit all required forms and information described in Exhibit A to the Purchasing Agent before providing Services.

1.2 General Contract Terms and Provisions. This Contract incorporates by reference the General Contract Terms and Provisions, attached hereto as Exhibit C.

1.3 Contract Administrator. The San Diego Police (Department) is the Contract Administrator for this Agreement. Contractor shall provide the Services under the direction of a designated representative of the Department as follows:

Lieutenant Steve Waldheim
1401 Broadway
San Diego, CA 92101
(619) 531-2143
swaldheim@pd.sandiego.gov

ARTICLE II
DURATION OF CONTRACT

2.1 Term. This Contract shall be for a period of five (5) years beginning on the Effective Date. The term of this Contract shall not exceed five years unless approved by the City Council by ordinance.

DOCUMENT NO. RR-315246
FILED DEC 05 2023
OFFICE OF THE CITY CLERK
SAN DIEGO, CALIFORNIA

ORIGINAL

2.2 Effective Date. This Contract shall be effective on the date it is executed by the last Party to sign the Contract, and approved by the City Attorney in accordance with San Diego Charter Section 40.

ARTICLE III
COMPENSATION

3.1 Amount of Compensation. City shall pay Contractor for performance of all Services rendered in accordance with this Contract in an amount not to exceed $12,099,384.45.

Contractor must immediately inform the City when the cumulative value of work done under this Agreement exceeds eighty percent (80%) of the total compensation authorized in this paragraph, or when it reasonably appears to Contractor that the cumulative value of work done under this Agreement may exceed the total compensation authorized in this paragraph within forty-five (45) days. The City is not required to pay more than the maximum amount authorized.

ARTICLE IV
WAGE REQUIREMENTS

4.1 Reserved.

ARTICLE V
CONTRACT DOCUMENTS

5.1 Contract Documents. The following documents comprise the Contract between the City and Contractor: this Contract and all exhibits thereto, the RFP; the Notice to Proceed; and the City's written acceptance of exceptions or clarifications to the RFP, if any.

5.2 Contract Interpretation. The Contract Documents completely describe the Services to be provided. Contractor will provide any Services that may reasonably be inferred from the Contract Documents or from prevailing custom or trade usage as being required to produce the intended result whether or not specifically called for or identified in the Contract Documents. Words or phrases which have a well-known technical or construction industry or trade meaning and are used to describe Services will be interpreted in accordance with that meaning unless a definition has been provided in the Contract Documents.

5.3 Precedence. In resolving conflicts resulting from errors or discrepancies in any of the Contract Documents, the Parties will use the order of precedence as set forth below. The 1st document has the highest priority. Inconsistent provisions in the Contract Documents that address the same subject, are consistent, and have different degrees of specificity, are not in conflict and the more specific language will control. The order of precedence from highest to lowest is as follows:

1st Any properly executed written amendment to the Contract

2nd The Contract

3rd The RFP and the City's written acceptance of any exceptions or clarifications to the RFP, if any

5.4 **Counterparts.** This Contract may be executed in counterparts which, when taken together, shall constitute a single signed original as though all Parties had executed the same page.

5.5 **Public Agencies.** Other public agencies, as defined by California Government Code section 6500, may choose to use the terms of this Contract, subject to Contractor's acceptance. The City is not liable or responsible for any obligations related to a subsequent Contract between Contractor and another public agency.

IN WITNESS WHEREOF, this Contract is executed by City and Contractor acting by and through their authorized officers.

CONTRACTOR

Axon Enterprise, Inc.
Proposer

17800 N. 85th Street
Street Address

Scottsdale, AZ 85255
City

800-978-2737
Telephone No.

contracts@axon.com
E-Mail

BY:
Signature of Proposer's Authorized Representative

Robert Driscoll
Print Name

VP, Associate General Counsel and Assistant Corporate Secretary
Title

08/11/2023
Date

CITY OF SAN DIEGO
A Municipal Corporation

BY:

Print Name: 12/21/23

~~Chief Financial Officer, Office of the Chief Financial Officer~~
Alia Khouri
Deputy Chief Operating Officer
General Services Branch

Date Signed

Approved as to form this 27 day of December, 2023.
MARA W. ELLIOTT, City Attorney

BY:
Deputy City Attorney

Lara Easton for DCA Jill Cristich

The City of
SAN DIEGO

November 22, 2023

VIA EMAIL TO: jgolish@axon.com

Mrs. Jaryna Golish, Associate Contracts Manager
Axon Enterprise, Inc.
17800 N 85th Street
Scottsdale, AZ 85255

Reference: Request for Proposal (RFP) No. 10090080-24-E, Body Worn Camera (BWC) System

Dear Mrs. Golish:

Subject: Exceptions Letter

Exhibit A, paragraph A.2.2 of the subject RFP, states, in pertinent part: "Any exceptions to the Contract that have not been accepted by the City in writing are deemed rejected. The City, in its sole discretion, may accept some or all of bidder's exceptions, reject bidder's exceptions and deem the bid non-responsive, or award the Contract without bidder's proposed exceptions."

This letter confirms our agreement to modify the terms of the Contract relating to the above-referenced solicitation. The Parties agree as follows:

1. The City accepts Axon's request to modify Article III of the agreement, Compensation. Section 3.1, subparagraph, and Article III of the General Terms and Provision, Compensation Section 3.1 shall be modified to the following:

   "Contractor must inform the City when it reasonably appears to Contractor that the cumulative value of work done under this Agreement may exceed the total compensation authorized in this paragraph within forty-five (45) days."

   "Manner of Payment. Contractor will invoice for payment of equipment upon delivery of goods and annually in advance for services provided in accordance with the terms and provisions specified in the Contract. Payment is due net 30 days from the invoice date. Payment obligations are non-cancelable. City will pay invoices without setoff, deduction, or withholding. City is responsible for sales and other taxes associated with the order unless City provides Contractor a valid tax exemption certificate".

2. The City rejects Axon's request to modify Exhibit B, Scope of Work, Section 13.

3. The City accepts Axon's request to modify Exhibit, C, City of San Diego General Terms and Provisions, Article I Scope and Term of Contract, Item 1.3 to include the following:

   "...described in the Contract. Any contract extension will be executed through a Bilateral contract amendment signed by both parties."

4. The City rejects Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE III Compensation, Item 3.26.

5. The City rejects Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE III Compensation, Item 3.4.

6. The City rejects Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE IV Suspension and Termination, Item 4.3.1.

7. The City accepts Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE IV Suspension and Termination, Item 4.3.2, shall be modified to the following:

   "If City Terminates this Contract, in whole or in part, City may procure, upon such terms and in such manner as the Purchasing Agent may deem appropriate, equivalent goods or services. Contractor shall also continue performance to the extent not terminated."

8. The City accepts Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE IV Suspension and Termination, is revised in part to include additional provisions:

   4.7 Contractor's Right to Termination. Contractor may terminate this Agreement for cause if it provides 60 days written notice of the breach to the City, and the breach remains uncured at the end of 60 days.

   4.7.1. Upon termination of this Contract for any reason, the City remains responsible for all fees incurred before the effective date of termination.

   4.7.2 If the City purchases Contractor hardware ("Devices") for less than the manufacturer's suggested retail price ("MSRP") and this Contract terminates before the end of the Term, Axon will invoice the City the difference between the MSRP for Devices received and amounts paid towards those Devices. Only if terminating for non-appropriation, the City may return Devices to Contractor within 30 days of termination. MSRP is the standalone price of the individual Device at the time of sale. For bundled Devices, MSRP is the stand-alone price of all individual components.

9. The City accepts Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE V Additional Contractor Obligations, Item 5.1, shall be modified to add the following:

"The City will inspect and accept goods provided under this Contract at the shipment destination unless specified otherwise. Inspection will be made and acceptance will be determined by the City department shown in the shipping address of the Purchase Order or other duly authorized representative of the City. City will provide Contractor with written notice of acceptance within 10 days of receipt of goods. Goods will be

deemed accepted if City does not provide Contractor with written notice within 10 days of receipt of goods.

10. The City accepts Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE V Additional Contractor Obligations, Item 5.7, is revised in part to include additional provisions to read:

Contractor warrants that Contractor-manufactured Devices are free from defects in workmanship and materials for 1 year from the date of City's receipt, except Signal Sidearm, which Contractor warrants for 30 months from the date of City's receipt. Contractor warrants its Contractor-manufactured accessories for 90 days from the date of City's receipt. Extended warranties run from the expiration of the 1-year hardware warranty through the extended warranty term. Non-Contractor manufactured Devices are not covered by Contractor's warranty. City should contact the manufacturer for support of non-Contractor manufactured Devices.

If Contractor receives a valid warranty claim for a Contractor manufactured Device during the warranty term, Contractor's sole responsibility is to repair or replace the Device with the same or like Device, at Contractor's option. A replacement Device will be new or like new. Contractor will warrant the replacement Device for the longer of (a) the remaining warranty of the original Device or (b) 90-days from the date of repair or replacement.

If City exchanges a device or part, the replacement item becomes City's property, and the replaced item becomes Contractor's property. Before delivering a Device for service, City must upload Device data to Contractor Evidence or download it and retain a copy. Contractor is not responsible for any loss of software, data, or other information contained in storage media or any part of the Device sent to Contractor for service.

Contractor may provide City a predetermined number of spare Devices as detailed in the Quote ("Spare Devices"). Spare Devices will replace broken or non-functioning units. If City utilizes a Spare Device, City must return to Contractor, through Contractor's warranty return process, any broken or nonfunctioning units. Contractor will repair or replace the unit with a replacement Device. Upon termination, Contractor will invoice City the MSRP then in effect for all Spare Devices provided. If City returns the Spare Devices to Contractor within 30 days of the invoice date, Contractor will issue a credit and apply it against the invoice.

Limitations. Contractor's warranty excludes damage related to: (a) failure to follow Device use instructions; (b) Devices used with equipment not manufactured or recommended by Contractor; (c) abuse, misuse, or intentional damage to Device; (d) force majeure; (e) Devices repaired or modified by persons other than Contractor without Contractor's written permission; or (f)Devices with a defaced or removed serial number.

To the extent permitted by law, the above warranties and remedies are exclusive. Contractor disclaims all other warranties, remedies, and conditions, whether oral, written, statutory, or implied. If statutory or implied warranties cannot be lawfully disclaimed, then such warranties are limited to the duration of the warranty described above and by the provisions in this Agreement.

Contractor's cumulative liability to any Party for any loss or damage resulting from any claim, demand, or action arising out of or relating to any Contractor Device or Service will not exceed the purchase price paid to Contractor for the Device, or if for Services, the amount paid for such Services over the 24 months preceding the claim. Neither Party will be liable for direct, special, indirect, incidental, punitive or consequential damages, however caused, whether for breach of warranty or contract, negligence, strict liability, tort or any other legal theory. The limitation on liability contained in this section does not apply to or in way limit Contractor's liability with regards to Contractor's gross negligence, fraud, or willful misconduct, nor shall it apply to Axon's indemnification obligations set forth in Article 7.1. In the event of any conflict between this section and Article 7.1, the language in Article 7.1 shall control. With respect to any data breach or data loss, Contractor's liability shall be limited to $5,000,000. Notwithstanding any limitation on liability contained herein, in the event Contractor's insurance would cover City's claim, City shall be able to recover up to the full value of Contractor's insurance coverage for any claim.

11. The City rejects Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE V Additional Contractor Obligations, Item 5.9.

12. The City accepts Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE VI Intellectual Property Right, is revised in part, to read as follows:

    6.1 Rights in Data. Contractor owns and reserves all right, title, and interest in Contractor devices and services and suggestions to Contractor, including all related intellectual property rights. City will not cause any Contractor proprietary rights to be violated.

    6. 2 Intellectual Property Warranty and Indemnification. Contractor represents and warrants that any materials or deliverables, including all Deliverable Materials, provided under this Contract are either original, or not encumbered, and do not infringe upon the copyright, trademark, patent or other intellectual property rights of any third party, or are in the public domain. If Deliverable Materials provided hereunder become the subject of a claim, suit or allegation of copyright, trademark or patent infringement, City shall have the right, in its sole discretion, to require Contractor to produce, at Contractor's own expense, new non-infringing materials, deliverables or works as a means of remedying any claim of infringement in addition to any other remedy available to the City under law or equity. Contractor further agrees to indemnify, defend, and hold harmless the City, its officers, employees and agents from and against any and all claims, actions, costs, judgments or damages, of any type, alleging or threatening that any Deliverable Materials, supplies, equipment, services or works provided under this contract infringe the copyright, trademark, patent or other intellectual property or proprietary rights of any third party (Third Party Claim of Infringement). City must promptly provide Contractor with written notice of such claim, tender to Contractor the defense or settlement of such claim at Contractor's expense and cooperate fully with Contractor in the defense or settlement

of such claim. Contractor acknowledges and agrees that any settlement is subject to approval by the City Council. Contractor's IP indemnification obligations do not apply

to claims based on (a) modification of Contractor Devices or Services by City or a third-party not approved by Contractor; (b) use of Contractor Devices and Services in combination with hardware or services not approved by Contractor; (c) use of Contractor Devices and Services other than as permitted in this Agreement; or (d) use of Contractor software that is not the most current release provided by Contractor.

6.3 Software Licensing. Contractor represents and warrants that the software, if any, as delivered to City, does not contain any program code, virus, worm, trap door, back door, time or clock that would erase data or programming or otherwise cause the software to become inoperable, inaccessible, or incapable of being used in accordance with its user manuals, either automatically, upon the occurrence of licensor-selected conditions or manually on command. Contractor further represents and warrants that all third party software, delivered to City or used by Contractor in the performance of the Contract, is fully licensed by the appropriate licensor.

6.4 Royalties, Licenses, and Patents. Unless otherwise specified, Contractor shall pay all royalties, license, and patent fees associated with the goods that are the subject of this solicitation. Contractor warrants that the goods, materials, supplies, and equipment to be supplied do not infringe upon any patent, trademark, or copyright, and further agrees to defend any and all suits, actions and claims for infringement that are brought against the City, and to defend, indemnify and hold harmless the City, its elected officials, officers, and employees from all liability, loss and damages, whether general, exemplary or punitive, suffered as a result of any actual or claimed infringement asserted against the City, Contractor, or those furnishing goods, materials, supplies, or equipment to Contractor under the Contract. City must promptly provide Contractor with written notice of such claim, tender to Contractor the defense or settlement of such claim at Contractor's expense and cooperate fully with Contractor in the defense or settlement of such claim. Contractor acknowledges and agrees that any settlement is subject to approval by the City Council. Contractor's IP indemnification obligations do not apply to claims based on (a) modification of Contractor Devices or Services by City or a third-party not approved by Contractor; (b) use of Contractor Devices and Services in combination with hardware or services not approved by Contractor; (c) use of Contractor Devices and Services other than as permitted in this Agreement; or (d) use of Contractor software that is not the most current release provided by Contractor.

13. The City accepts Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE VII Indemnification and Insurance, Item 7.1, is revised in part, to read as follows:

To the fullest extent permitted by law, Contractor shall defend (with legal counsel reasonably acceptable to City), indemnify, protect, and hold harmless City and its elected officials, officers, employees, agents, and representatives (Indemnified Parties) from and against any and all claims, losses, costs, damages, injuries (including, without limitation, injury to or death of an employee of Contractor or its subcontractors), expenses, and liability of every kind, nature and description (including, without limitation, incidental and consequential damages, court costs, and litigation expenses and fees of expert consultants or expert witnesses incurred in

connection therewith and costs of investigation) that arise out of, pertain to, or relate to, directly or indirectly, in whole or in part any third party claim against an Indemnified Party relating to the negligent act, error or omission, or willful misconduct of Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or anyone that either of them control under this, any goods provided or performance of services under this Contract by Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or anyone that either of them control. Contractor's duty to defend, indemnify, protect and hold harmless shall not include any claims or liabilities arising from the sole negligence or willful misconduct of the Indemnified Parties. If judgment is entered against Contractor and the City by a court of competent jurisdiction because of the concurrent active negligence of County or the City Indemnitees, Contractor and the City agree that liability will be apportioned as determined by the court.

14. The City accepts Axon's request to delete Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE VIII Bonds.

    8.1 Reserved.

    8.2 Reserved.

15. The City rejects Axon's request to modify Exhibit C, City of San Diego General Contract Terms and Provisions, ARTICLE XIII Miscellaneous, Item 13.2.

Please indicate your agreement with the above by signing the bottom of this letter. Thank you for your assistance.

Sincerely,

William Eames III
William Eames III
Supervising Procurement Contracting Officer
Purchasing & Contracting

This Letter is executed by the City and Contractor acting by and through their authorized officers.

AXON ENTERPRISE, INC.	THE CITY OF SAN DIEGO
By: Robert E. Driscoll, Jr. (Robert E. Driscoll, Jr. (Nov 27, 2023 13:03 MST))	By:
Name: Robert E. Driscoll, Jr.	Name: Claudia C. Abarca
Title: VP, Associate General Counsel	Title: Director, Purchasing & Contracting
Date: Nov 27, 2023	Date: December 19, 2023

R-315246

City of San Diego - RFP 10090080-24-E, Body Worn Cameras

Final Audit Report 2023-11-27

Created:	2023-11-27
By:	William Eames III (wbeames@sandiego.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAACKJYlrLdeApbvHIvV9GFzPXKAG1SKNZi

"City of San Diego - RFP 10090080-24-E, Body Worn Cameras" History

Document created by William Eames III (wbeames@sandiego.gov)
2023-11-27 - 5:34:28 PM GMT

Document emailed to bobby@axon.com for signature
2023-11-27 - 5:36:26 PM GMT

Email viewed by bobby@axon.com
2023-11-27 - 5:48:30 PM GMT

Signer bobby@axon.com entered name at signing as Robert E. Driscoll, Jr.
2023-11-27 - 8:03:57 PM GMT

Document e-signed by Robert E. Driscoll, Jr. (bobby@axon.com)
Signature Date: 2023-11-27 - 8:03:59 PM GMT - Time Source: server

Agreement completed.
2023-11-27 - 8:03:59 PM GMT

EXHIBIT A
PROPOSAL SUBMISSION AND REQUIREMENTS

A. PROPOSAL SUBMISSION

1. Timely Proposal Submittal. Proposals must be submitted as described herein to the Purchasing & Contracting Department (P&C).

1.1 Reserved.

1.2 Paper Proposals. The City will accept paper proposals in lieu of eProposals. Paper proposals must be submitted in a sealed envelope to the Purchasing & Contracting Department (P&C) located at 1200 Third Avenue, Suite 200, San Diego, CA 92101. The Solicitation Number and Closing Date must be referenced in the lower left-hand corner of the outside of the envelope. Faxed proposals will not be accepted.

1.3 Proposal Due Date. Proposals must be submitted prior to the Closing Date indicated on the eBidding System. E-mailed and/or faxed proposals will not be accepted.

1.4 Pre-Proposal Conference. No pre-proposal conference will be held for RFP.

1.4.1 Reserved.

1.5 Questions and Comments. Written questions and comments must be submitted electronically via the eBidding System no later than the date specified on the eBidding System. Only written communications relative to the procurement shall be considered. The City's eBidding System is the only acceptable method for submission of questions. All questions will be answered in writing. The City will distribute questions and answers without identification of the inquirer(s) to all proposers who are on record as having received this RFP, via its eBidding System. No oral communications can be relied upon for this RFP. Addenda will be issued addressing questions or comments that are determined by the City to cause a change to any part of this RFP.

1.6 Contact with City Staff. Unless otherwise authorized herein, proposers who are considering submitting a proposal in response to this RFP, or who submit a proposal in response to this RFP, are prohibited from communicating with City staff about this RFP from the date this RFP is issued until a contract is awarded.

2. Proposal Format and Organization. Unless electronically submitted, all proposals should be securely bound and must include the following completed and executed forms and information presented in the manner indicated below:

Tab A - Submission of Information and Forms.

2.1 Completed and signed Contract Signature Page. If any addenda are issued, the latest Addendum Contract Signature Page is required.

2.2 Exceptions requested by proposer, if any. The proposer must present written factual or legal justification for any exception requested to the Scope of Work, the Contract, or the Exhibits thereto. Any exceptions to the Contract that have not been accepted

by the City in writing are deemed rejected. The City, in its sole discretion, may accept some or all of proposer's exceptions, reject proposer's exceptions, and deem the proposal non-responsive, or award the Contract without proposer's proposed exceptions. The City will not consider exceptions addressed elsewhere in the proposal.

2.3 The Contractor Standards Pledge of Compliance Form.

2.4 Equal Opportunity Contracting forms including the Work Force Report and Contractors Certification of Pending Actions.

2.5 Reserved.

2.6 Reserved.

2.7 Reserved.

2.8 Additional Information as required in Exhibit B.

2.9 Reserved.

Tab B - Executive Summary and Responses to Specifications.

2.10 A title page.

2.11 A table of contents.

2.12 An executive summary, limited to one typewritten page, that provides a high-level description of the proposer's ability to meet the requirements of the RFP and the reasons the proposer believes itself to be best qualified to provide the identified services.

2.13 Proposer's response to the RFP.

Tab C - Cost/Price Proposal (if applicable). Proposers shall submit a cost proposal in the form and format described herein. Failure to provide cost(s) in the form and format requested may result in proposal being declared non-responsive and rejected.

3. Proposal Review. Proposers are responsible for carefully examining the RFP, the Specifications, this Contract, and all documents incorporated into the Contract by reference before submitting a proposal. If selected for award of contract, proposer shall be bound by same unless the City has accepted proposer's exceptions, if any, in writing.

4. Addenda. The City may issue addenda to this RFP as necessary. All addenda are incorporated into the Contract. The proposer is responsible for determining whether addenda were issued prior to a proposal submission. Failure to respond to or properly address addenda may result in rejection of a proposal.

5. Quantities. The estimated quantities provided by the City are not guaranteed. These quantities are listed for informational purposes only. Quantities vary depending on the demands of the City. Any variations from the estimated quantities shall not entitle the proposer to an adjustment in the unit price or any additional compensation.

6. Reserved.

7. Modifications, Withdrawals, or Mistakes. Proposer is responsible for verifying all prices and extensions before submitting a proposal.

7.1 Modification or Withdrawal of Proposal Before Proposal Opening. Prior to the Closing Date, the proposer or proposer's authorized representative may modify or withdraw the proposal by providing written notice of the proposal modification or withdrawal to the City Contact via the eBidding System. E-mail or telephonic withdrawals or modifications are not permissible.

7.2 Proposal Modification or Withdrawal of Proposal After Proposal Opening. Any proposer who seeks to modify or withdraw a proposal because of the proposer's inadvertent computational error affecting the proposal price shall notify the City Contact identified on the eBidding System no later than three working days following the Closing Date. The proposer shall provide worksheets and such other information as may be required by the City to substantiate the claim of inadvertent error. Failure to do so may bar relief and allow the City recourse from the bid surety. The burden is upon the proposer to prove the inadvertent error. If, as a result of a proposal modification, the proposer is no longer the apparent successful proposer, the City will award to the newly established apparent successful proposer. The City's decision is final.

8. Incurred Expenses. The City is not responsible for any expenses incurred by proposers in participating in this solicitation process.

9. Public Records. By submitting a proposal, the proposer acknowledges that any information submitted in response to this RFP is a public record subject to disclosure unless the City determines that a specific exemption in the California Public Records Act (CPRA) applies. If the proposer submits information clearly marked confidential or proprietary, the City may protect such information and treat it with confidentiality to the extent permitted by law. However, it will be the responsibility of the proposer to provide to the City the specific legal grounds on which the City can rely in withholding information requested under the CPRA should the City choose to withhold such information. General references to sections of the CPRA will not suffice. Rather, the proposer must provide a specific and detailed legal basis, including applicable case law, that clearly establishes the requested information is exempt from the disclosure under the CPRA. If the proposer does not provide a specific and detailed legal basis for requesting the City to withhold proposer's confidential or proprietary information at the time of proposal submittal, City will release the information as required by the CPRA and proposer will hold the City, its elected officials, officers, and employees harmless for release of this information. It will be the proposer's obligation to defend, at proposer's expense, any legal actions or challenges seeking to obtain from the City any information requested under the CPRA withheld by the City at the proposer's request. Furthermore, the proposer shall indemnify and hold harmless the City, its elected officials, officers, and employees from and against any claim or liability, and defend any action brought against the City, resulting from the City's refusal to release information requested under the CPRA which was withheld at proposer's request. Nothing in the Contract resulting from this proposal creates any obligation on the part of the City to notify the proposer or obtain the proposer's approval or consent before releasing information subject to disclosure under the CPRA.

10. Right to Audit. The City Auditor may access proposer's records as described in San Diego Charter section 39.2 to confirm contract compliance.

B. PRICING

1. Fixed Price. All prices shall be firm, fixed, fully burdened, FOB destination, and include any applicable delivery or freight charges, and any other costs required to provide the requirements as specified in this RFP. The lowest total estimated contract price of all the proposals that meet the requirements of this RFP will receive the maximum assigned points to this category as set forth in this RFP. The other price schedules will be scored based on how much higher their total estimated contract prices compare with the lowest:

$$\left(1 - \frac{\text{(contract price - lowest price)}}{\text{lowest price}}\right) \times \text{maximum points} = \text{points received}$$

For example, if the lowest total estimated contract price of all proposals is $100, that proposal would receive the maximum allowable points for the price category. If the total estimated contract price of another proposal is $105 and the maximum allowable points is 60 points, then that proposal would receive (1 – ((105 – 100) / 100) x 60 = 57 points, or 95% of the maximum points. The lowest score a proposal can receive for this category is zero points (the score cannot be a negative number). The City will perform this calculation for each Proposal.

2. Taxes and Fees. Taxes and applicable local, state, and federal regulatory fees should not be included in the price proposal. Applicable taxes and regulatory fees will be added to the net amount invoiced. The City is liable for state, city, and county sales taxes but is exempt from Federal Excise Tax and will furnish exemption certificates upon request. All or any portion of the City sales tax returned to the City will be considered in the evaluation of proposals.

3. Escalation. An escalation factor is not allowed unless called for in this RFP. If escalation is allowed, proposer must notify the City in writing in the event of a decline in market price(s) below the proposal price. At that time, the City will make an adjustment in the Contract or may elect to re-solicit.

4. Unit Price. Unless the proposer clearly indicates that the price is based on consideration of being awarded the entire lot and that an adjustment to the price was made based on receiving the entire proposal, any difference between the unit price correctly extended and the total price shown for all items shall be offered shall be resolved in favor of the unit price.

C. EVALUATION OF PROPOSALS

1. Award. The City shall evaluate each responsive proposal to determine which proposal offers the City the best value consistent with the evaluation criteria set forth herein. The proposer offering the lowest overall price will not necessarily be awarded a contract.

2. Sustainable Materials. Consistent with Council Policy 100-14, the City encourages use of readily recyclable submittal materials that contain post-consumer recycled content.

3. Evaluation Process.

3.1 Process for Award. A City-designated evaluation committee (Evaluation Committee) will evaluate and score all responsive proposals. The Evaluation Committee may require proposer to provide additional written or oral information to clarify responses. Upon completion of the evaluation process, the Evaluation Committee will recommend to the Purchasing Agent that award be made to the proposer with the highest scoring proposal.

3.2 Reserved.

3.3 Mandatory Interview/Demo The City will require proposers to interview and/or make an oral presentation if one or more proposals score within seven (7) points or less of the proposal with the highest score. Only the proposer with the highest scoring proposal and those proposers scoring within seven (7) points or less of the highest scoring proposal will be asked to interview and/or make an oral presentation. Interviews and/or oral presentations will be made to the Evaluation Committee in order to clarify the proposals and to answer any questions. The interviews and/or oral presentations will be scored as part of the selection process. The City will complete all reference checks prior to any oral interview. Additionally, the Evaluation Committee may require proposer's key personnel to interview. Interviews may be by telephone and/or in person. Multiple interviews may be required. Proposers are required to complete their oral presentation and/or interviews within seven (7) workdays after the City's request. Proposers should be prepared to discuss and substantiate any of the areas of the proposal submitted, as well as proposer's qualifications to furnish the subject goods and services. Proposer is responsible for any costs incurred for the oral presentation and interview of the key personnel.

3.4 Discussions/Negotiations. The City has the right to accept the proposal that serves the best interest of the City, as submitted, without discussion or negotiation. Contractors should, therefore, not rely on having a chance to discuss, negotiate, and adjust their proposals. The City may negotiate the terms of a contract with the winning proposer based on the RFP and the proposer's proposal, or award the contract without further negotiation.

3.5 Inspection. The City reserves the right to inspect the proposer's equipment and facilities to determine if the proposer is capable of fulfilling this Contract. Inspection will include, but not limited to, survey of proposer's physical assets and financial capability. Proposer, by signing the proposal agrees to the City's right of access to physical assets and financial records for the sole purpose of determining proposer's capability to perform the Contract. Should the City conduct this inspection, the City reserves the right to disqualify a proposer who does not, in the City's judgment, exhibit the sufficient physical and financial resources to perform this Contract.

[Remainder of page intentionally left blank]

3.6 Evaluation Criteria. The following elements represent the evaluation criteria that will be considered during the evaluation process:

	MAXIMUM EVALUATION POINTS
A. Responsiveness to the RFP 1. Requested information included and thoroughness of response. 2. Understanding of the RFP and ability to deliver.	**15**
B. Staffing Plan. 1. Qualifications of personnel adequate for requirement. 2. Availability/Geographical location of personnel for required tasks 3. Clearly defined Roles/Responsibilities of personnel.	**15**
C. Proposer's Capability to provide the Service, Expertise and Past Performance. 1. Relevant experience of the Proposer 2. Financial stability 3. Litigation 4. Equipment, video management, storage capabilities 5. Proposer's training ability and experience 6. Ability to meet The City of San Diego needs in a timely manner 7. Reference checks	**45**
D. Price.	**10**
E. Mandatory Interview/Demo (if held pursuant to Section 3.3 above) at no cost to the City. 1. Equipment 2. Software 3. Support Model 4. Implementation Outline 5. Thoroughness and Clarity of Presentation	**15**
SUB TOTAL MAXIMUM EVALUATION POINTS:	**100**
F. Participation by Small Local Business Enterprise (SLBE) or Emerging Local Business Enterprise (ELBE) Firms*	**12**
FINAL MAXIMUM EVALUATION POINTS INCLUDING SLBE/ELBE:	**112**

*The City shall apply a maximum of an additional 12 percentage points to the proposer's final score for SLBE OR ELBE participation. Refer to Equal Opportunity Contracting Form, Section V.

D. ANNOUNCEMENT OF AWARD

1. Award of Contract. The City will inform all proposers of its intent to award a Contract in writing.

2. **Obtaining Proposal Results**. No solicitation results can be obtained until the City announces the proposal or proposals best meeting the City's requirements. Proposal results may be obtained by: (1) e-mailing a request to the City Contact identified on the eBidding System or (2) visiting the P&C eBidding System to review the proposal results. To ensure an accurate response, requests should reference the Solicitation Number. Proposal results will not be released over the phone.

3. **Multiple Awards.** City may award more than one contract by awarding separate items or groups of items to various proposers. Awards will be made for items, or combinations of items, which result in the lowest aggregate price and/or best meet the City's requirements. The additional administrative costs associated with awarding more than one Contract will be considered in the determination.

E. PROTESTS. The City's protest procedures are codified in Chapter 2, Article 2, Division 30 of the San Diego Municipal Code (SDMC). These procedures provide unsuccessful proposers with the opportunity to challenge the City's determination on legal and factual grounds. The City will not consider or otherwise act upon an untimely protest.

F. SUBMITTALS REQUIRED UPON NOTICE TO PROCEED. The successful proposer is required to submit the following documents to P&C **within ten (10) business days** from the date on the Notice to Proceed letter:

1. **Insurance Documents.** Evidence of all required insurance, including all required endorsements, as specified in Article VII of the General Contract Terms and Provisions.

2. **Taxpayer Identification Number.** Internal Revenue Service (IRS) regulations require the City to have the correct name, address, and Taxpayer Identification Number (TIN) or Social Security Number (SSN) on file for businesses or persons who provide goods or services to the City. This information is necessary to complete Form 1099 at the end of each tax year. To comply with IRS regulations, the City requires each Contractor to provide a Form W-9 prior to the award of a Contract.

3. **Business Tax Certificate.** Unless the City Treasurer determines a business is exempt, all businesses that contract with the City must have a current business tax certificate.

4. **Reserved.**

5. **Reserved.**

The City may find the proposer to be non-responsive and award the Contract to the next highest scoring responsible and responsive proposer if the apparent successful proposer fails to timely provide the required information or documents.

EXHIBIT B
SCOPE OF WORK

A. SPECIFICATIONS

1. Background

The San Diego Police Department (SDPD) has over 1,800 sworn law enforcement officers serving a diverse city of over 1.4 million residents. SDPD strives to advance the highest levels of public safety, trust, and professionalism by strengthening community partnerships through fair and impartial policing while fostering employee enrichment and growth to ensure we remain America's finest police department. The use of body worn cameras (BWCs) has proven effective in reducing violent confrontations and complaints against officers. Cameras provide additional documentation of police/public encounters and are an important tool for collecting evidence and maintaining public trust. The San Diego Police Department currently has over 2,200 BWCs produced by Axon Enterprise, Inc. in service and assigned to Department members.

2. Statement of Work.

The City of San Diego (City) is soliciting proposals from qualified contractors to provide a user-friendly, cloud based BWC System Solution. The BWC System Solution shall be a tool to demonstrate SDPD's commitment to transparency, ensure the accountability of its members, increase the public's trust in officers, and protect its members from unjustified complaints of misconduct. The purpose of this solicitation is to outfit current employees as well as recruits graduating the Academy (2,250 initial delivery and approximately 200 additional each year to account for academy graduations).

The successful Proposer will be expected to provide the City with a complete BWC System Solution that will include the following: Body Worn Cameras (hardware), Video Management/Storage, licensing, configuration, implementation, training services and ongoing maintenance support services for hardware and software, throughout the term of the contract.

Proposers providing partial solutions (e.g. storage only or hardware only) will not be considered for contract award and will be deemed non-responsive.

Services will commence on, or about, January 1, 2024. Its is the City's intent to place as-needed orders for the following equipment, as described in the Specifications, starting at the earliest part of the first year of this contract with an option to purchase additional equipment over the term of this contract. Proposals that do not meet all of

the specifications for all of the BWC's, associated equipment and services may be rejected as non-responsive.

As an example, the City provides in Table 1 an estimate of BWCs proposed by SDPD.

Table 1

Year 1	Year 2	Year 3	Year 4	Year 5
2250	200	200	200	200

The estimated annual quantities are not guaranteed, and actual purchases may vary depending on the demands of the City. Any variations from the estimated quantities shall not entitle the proposer to an adjustment in the unit price or any additional compensation.

In addition to the cameras, the City will be purchasing the necessary mounting systems, docking solutions, as well as licensing, storage, and video management software. The City reserves the right to request equipment and services as-and-when required throughout the duration of the contract.

3. **Experience.**

Briefly, as an overview, Proposer shall describe their experience in providing the goods and services described in this RFP. Proposer shall have a minimum of five (5) years of verifiable experience in delivering and currently maintaining BWC, Video Management, and Storage solutions. Proposers shall provide a list of a minimum of three (3) references of law enforcement agencies where you have provided similar services with at least 1,500 BWCs for each agency.

4. **Financials.**

Proposers shall provide documentation to support your organization's financial stability and ability to maintain the program throughout the contract period. Documentation may include cash and/or credit reserves. In addition, the proposer shall provide the following information for the last three (3) fiscal years:

1. Statement of Financial Position (Balance Sheet);
2. Statement of Activities (Income Statement); and
3. Statement of Cash Flow

5. **Litigation.**

Proposer shall provide the status of any lawsuits and/or pending litigation that involve failure to deliver performance on similar scope contracts and/or lawsuits/litigation that directly impact this contract (i.e., technology patents, etc.). Provide information regarding status, resolutions, and if any penalties, fines, or other actions required.

6. **BWC Specifications.**

The proposer must meet the following specifications and requirements:

Hardware Technical Specifications:

1. All BWCs must be factory new with no previous owner. They shall be the latest model in current production or, if multiple models are available, the model chosen by the City.
2. BWC must attach to the chest/upper torso area (patrol and investigations).
3. Smaller cameras capable of being attached to specialized unit helmets must be available.
4. BWC must be functional in all potential operating temperatures in San Diego County.
5. BWC must be functional in relative humidity up to 80% (non-condensing).
6. BWC must have an estimated useful life: Approximately 5 years.
7. BWC will have a rechargeable lithium-ion battery or similar capable of lasting at least a working shift of 12 hours on a single charge.
8. BWC must have multiple microphones built into the camera for clearer sound.
9. BWC must be available with a variety of mounts to attach to uniforms or other equipment including MOLLE mounts.
10. BWC must be Bluetooth and Wi-Fi enabled.
11. BWC must have at least 64 GB of internal memory.
12. All BWCs must have a full replacement warranty of at least 1 year.
13. BWC must have the capability to attach camera accessories fitting a wide range of mounts for special purpose units.

Software Technical Specifications:

1. BWC must be a full color audio/video camera.
2. Ability to record in multiple color video resolutions that can be selected by the City.
3. Pre-event audio/video buffer that is configurable by the City.
4. BWC must be able to effectively record in low-light conditions.
5. The image field of view must be at least 65 degrees vertical, 120 degrees horizontal and 140 degrees diagonal.
6. BWC must be encrypted.
7. BWC should have immediate playback capability via a separate viewer/smart device/cell phone application.

Design Requirements:

1. BWC shall be ruggedized and constructed of a highly durable material.
2. The City's BWC color preference is black.
3. The BWC will be no more than 4" in height.
4. The BWC will be no more than 3" wide.
5. The BWC will be no more than 1.5" in depth.
6. The BWC will be of a weight that does not impede the officer from engaging in normal police activities.
7. The BWC will have a large on/off button to start/stop recording.
8. The BWC will have an indicator light to show operational status of the camera.

9. The BWC will have a display screen which will minimally indicate the battery status and recording status of the camera.
10. BWC shall have an audible chime/beep that sounds intermittently to notify the user that they are in recording mode. The user must be able to control the volume level of this notification including turning it off so they are in "stealth mode."

7. **Docking Station Specifications.**

The proposer must meet the following docking station specifications:

1. Availability of multiple docking options including multiple bay and single bay docks.
2. Primary video upload method must be via a docking station which allows BWC to upload videos and charge its battery at the same time.
3. Attachment to a computer cannot be the primary method of uploading videos.

8. **Video Management/Storage System Specifications.**

The proposer must meet the following video management system specifications:

1. Unlimited video storage.
2. User-friendly video management system.
3. Ability to export video in an industry standard file format.
4. Acknowledgment that all data is property of the City and must be made available at no additional cost.
5. Storage solution compliance with policies outlined in the U.S. Department of Justice Information Services (CJIS) Security Policy and the City of San Diego Information Security Standards and Guidelines. See attached links for further information. CJIS Security Policy 2022 v5.9.1 — FBI. Microsoft Word - AR_90-63_Information_Security_FINAL_2011-06-28.docx (sandiego.gov).
6. Capability to produce digitally authenticated duplicates.
7. Cloud-based storage.
8. Ability for retrieve/search video footage.
9. Comprehensive metadata storage capability.
10. Storage system must be able to quickly extract segments of needed footage.
11. Audit trail capability.
12. Ability for video management administrator to assign different access roles based on user's assignment.
13. Users must be able to attach data to the videos in the field. Data is used to make videos searchable.
14. System must be capable of accepting photos in addition to videos.
15. System must have file and case sharing capabilities.
16. Ability for automatic file deletion schedules in addition to the ability of the administrator to change the preset schedules.
17. Videos should be watermarked for security purposes.
18. Ability for customizable reports/logs.
19. System must be capable of allowing victims/witnesses/citizens to upload videos at the request of investigators.

9. **Additional Available Features.**

   The proposer must have the following additional add-on features available for purchase by the City:

   1. Ability for event data to automatically be added to each video based on integration with City's CAD vendor Hexagon (auto tagging).
   2. Video redaction capabilities to include audio and video.
   3. Live feed from multiple cameras that are in record mode.
   4. Automatic "on" activation feature.

10. **Pricing Schedule.**

    Proposers shall submit their pricing in Attachment 1 of Section C in the following manner:

    1. The Proposer should carefully review this RFP and address all items and services in their proposed fee structure and schedule.
    2. If a Proposer identifies a package solution(s), the details of what is included in the package (hardware, storage, licensing, etc.) should be listed in the appropriate section of the Pricing Schedule and the cost listed on a per camera basis.
    3. Unit price will be used to evaluate proposals for pricing in accordance with section 3.6 of Exhibit A of this RFP.
    4. Award shall be made to a single proposer. Proposer is required to submit pricing for each line item listed in Pricing Pages-Exhibit B, Attachment 1. Proposers may submit additional pricing for Price Schedules and bundles. Pricing Pages-Exhibit B, Attachment 1 will be used to evaluate proposals for pricing in accordance with Section 3.6 of Exhibit A of this RFP. (Other Price Schedules or bundles shall not be included in the evaluation for award)
    5. Any deviations from the Price Schedule may result in a proposal being rejected as non-responsive. The Pricing Page is the only form and format that will be accepted for proposal pricing.
    6. Blanks on the pricing pages will be interpreted as zero (0).

11. **Training Requirements.**

    1. All training listed below (2-5) will be provided at no additional cost to the City.
    2. Provide on-site instructor certification training for San Diego Police Department Operational Support Administration personnel. If new models of BWCs are released by the successful proposer and purchased by the Department throughout the duration of the proposed contract, the successful proposer shall provide updated instructor certification training for San Diego Police Department Operational Support Administration personnel.
    3. Provide on-site training for City and Department technical staff as it relates to video management and storage system specifications.
    4. San Diego Police Department Operational Support Administration personnel shall be recognized by the successful proposer as certified BWC instructors for the Department.

5. All Department personnel trained by the San Diego Police Operational Support Administration in the use of the BWC shall be recognized by the successful proposer as being properly and sufficiently trained in the use of the BWC.
6. All initial training must be completed within 30 days of the execution of the contract.

12. **Security and Privacy.**

The successful Proposer (Awardee) shall at all times use its best efforts but in no event less than current industry best practices to protect the security and privacy of all City data where "security" is defined as protection of software and data from natural and human-caused hazards, and where "privacy" is defined as protection of software and data from unauthorized access and manipulation. Proposer shall also assure integrity of data by establishing and maintaining safeguards against the destruction, loss, or unauthorized alteration of City's data. Proposer shall, to the greatest extent possible, prevent security and privacy breaches, to address contingencies in the event of an unavoidable security or privacy breach, and to provide recovery and backup operation. Proposer shall comply with all security rules and regulations as it pertains to the San Diego Police Department and City of San Diego.

Criminal Justice Information Services (CJIS) Security Policy. Contractor acknowledges and shall comply with the requirements in U.S. Department of Justice, Federal Bureau of Investigation, (CJIS) Security Policy. A copy of (CJIS) Security Policy is attached as Attachment II to the Contract and is incorporated herein by reference.

City IT Standards and Guidelines. Contractor acknowledges and shall comply with the requirements in City of San Diego IT Standards and Guideline. A copy of IT is attached as Attachment III to the Contract and is incorporated herein by reference.

13. **Subcontractors.**

Proposer shall not use Subcontractors to provide any labor, facilities, equipment, accessories, tools and other items and do any work required under the Scope of Work unless expressly agreed to by City in writing.

14. **Delivery**

All deliverables described in this Scope of Work and training requirements **must be completed within 30 days** of execution of the contract. However, the City will consider and evaluate timelines submitted that exceed the 30-day timeline.

All deliveries under this contract shall be made to San Diego Police Department Headquarters located at:

San Diego Police Department – Operational Support
1401 Broadway
San Diego, CA 92101

15. **Returns**

Returns of inoperable and/or damaged equipment will be returned to the successful Proposer at no cost to the City.

B. CONTRACT ADMINISTRATOR

The Contract Administrator for this Contract is identified in the notice of intent to award and will provide daily oversight of this Contract to ensure compliance to the scope of work and performance to Contract specifications. The Technical Representative, or designee, is also responsible for oversight of all invoice payments and billing questions for purchase orders issued under this Contract.

C. PRICING SCHEDULE

Proposers must provide pricing for the goods and services described in Exhibit B – Attachment 1 Pricing Schedule. The estimated quantities are provided in Table 1 in Section 2 of Exhibit B Scope of Work. The estimated quantities are not guaranteed, and actual purchases will vary depending on the demands of the City.

EXHIBIT C

THE CITY OF SAN DIEGO

GENERAL CONTRACT TERMS AND PROVISIONS

APPLICABLE TO GOODS, SERVICES, AND CONSULTANT CONTRACTS

ARTICLE I
SCOPE AND TERM OF CONTRACT

1.1 Scope of Contract. The scope of contract between the City and a provider of goods and/or services (Contractor) is described in the Contract Documents. The Contract Documents are comprised of the Request for Proposal, Invitation to Bid, or other solicitation document (Solicitation); the successful bid or proposal; the letter awarding the contract to Contractor; the City's written acceptance of exceptions or clarifications to the Solicitation, if any; and these General Contract Terms and Provisions.

1.2 Effective Date. A contract between the City and Contractor (Contract) is effective on the last date that the contract is signed by the parties and approved by the City Attorney in accordance with Charter section 40. Unless otherwise terminated, this Contract is effective until it is completed or as otherwise agreed upon in writing by the parties, whichever is the earliest. A Contract term cannot exceed five (5) years unless approved by the City Council by ordinance.

1.3 Contract Extension. The City may, in its sole discretion, unilaterally exercise an option to extend the Contract as described in the Contract Documents. In addition, the City may, in its sole discretion, unilaterally extend the Contract on a month-to-month basis following contract expiration if authorized under Charter section 99 and the Contract Documents. Contractor shall not increase its pricing in excess of the percentage increase described in the Contract.

ARTICLE II
CONTRACT ADMINISTRATOR

2.1 Contract Administrator. The Purchasing Agent or designee is the Contract Administrator for purposes of this Contract, and has the responsibilities described in this Contract, in the San Diego Charter, and in Chapter 2, Article 2, Divisions 5, 30, and 32.

2.1.1 Contractor Performance Evaluations. The Contract Administrator will evaluate Contractor's performance as often as the Contract Administrator deems necessary throughout the term of the contract. This evaluation will be based on criteria including the quality of goods or services, the timeliness of performance, and adherence to applicable laws, including prevailing wage and living wage. City will provide Contractors who receive an unsatisfactory rating with a copy of the evaluation and an opportunity to respond. City may consider final evaluations, including Contractor's response, in evaluating future proposals and bids for contract award.

2.2 Notices. Unless otherwise specified, in all cases where written notice is required under this Contract, service shall be deemed sufficient if the notice is personally delivered or deposited in the United States mail, with first class postage paid, attention to the Purchasing Agent. Proper notice is effective on the date of personal delivery or five (5) days after deposit in a United States postal mailbox unless provided otherwise in the Contract. Notices to the City shall be sent to:

Purchasing Agent
City of San Diego, Purchasing and Contracting Division
1200 3rd Avenue, Suite 200
San Diego, CA 92101-4195

ARTICLE III
COMPENSATION

3.1 Manner of Payment. Contractor will be paid monthly, in arrears, for goods and/or services provided in accordance with the terms and provisions specified in the Contract.

3.2 Invoices.

3.2.1 Invoice Detail. Contractor's invoice must be on Contractor's stationary with Contractor's name, address, and remittance address if different. Contractor's invoice must have a date, an invoice number, a purchase order number, a description of the goods or services provided, and an amount due.

3.2.2 Service Contracts. Contractor must submit invoices for services to City by the 10th of the month following the month in which Contractor provided services. Invoices must include the address of the location where services were performed and the dates in which services were provided.

3.2.3 Goods Contracts. Contractor must submit invoices for goods to City within seven days of the shipment. Invoices must describe the goods provided.

3.2.4 Parts Contracts. Contractor must submit invoices for parts to City within seven calendar (7) days of the date the parts are shipped. Invoices must include the manufacturer of the part, manufacturer's published list price, percentage discount applied in accordance with Pricing Page(s), the net price to City, and an item description, quantity, and extension.

3.2.5 Extraordinary Work. City will not pay Contractor for extraordinary work unless Contractor receives prior written authorization from the Contract Administrator. Failure to do so will result in payment being withheld for services. If approved, Contractor will include an invoice that describes the work performed and the location where the work was performed, and a copy of the Contract Administrator's written authorization.

3.2.6 Reporting Requirements. Contractor must submit the following reports using the City's web-based contract compliance portal. Incomplete and/or delinquent reports may cause payment delays, non-payment of invoice, or both. For questions, please view the City's online tutorials on how to utilize the City's web-based contract compliance portal.

3.2.6.1 Monthly Employment Utilization Reports. Contractor and Contractor's subcontractors and suppliers must submit Monthly Employment Utilization Reports by the fifth (5th) day of the subsequent month.

3.2.6.2 Monthly Invoicing and Payments. Contractor and Contractor's subcontractors and suppliers must submit Monthly Invoicing and Payment Reports by the fifth (5^{th}) day of the subsequent month.

3.3 Annual Appropriation of Funds. Contractor acknowledges that the Contract term may extend over multiple City fiscal years, and that work and compensation under this Contract is contingent on the City Council appropriating funding for and authorizing such work and compensation for those fiscal years. This Contract may be terminated at the end of the fiscal year for which sufficient funding is not appropriated and authorized. City is not obligated to pay Contractor for any amounts not duly appropriated and authorized by City Council.

3.4 Price Adjustments. Based on Contractor's written request and justification, the City may approve an increase in unit prices on Contractor's pricing pages consistent with the amount requested in the justification in an amount not to exceed the increase in the Consumer Price Index, San Diego Area, for All Urban Customers (CPI-U) as published by the Bureau of Labor Statistics, or 5.0%, whichever is less, during the preceding one year term. If the CPI-U is a negative number, then the unit prices shall not be adjusted for that option year (the unit prices will not be decreased). A negative CPI-U shall be counted against any subsequent increases in the CPI-U when calculating the unit prices for later option years. Contractor must provide such written request and justification no less than sixty days before the date in which City may exercise the option to renew the contract, or sixty days before the anniversary date of the Contract. Justification in support of the written request must include a description of the basis for the adjustment, the proposed effective date and reasons for said date, and the amount of the adjustment requested with documentation to support the requested change (e.g. CPI-U or 5.0%, whichever is less). City's approval of this request must be in writing.

ARTICLE IV
SUSPENSION AND TERMINATION

4.1 City's Right to Suspend for Convenience. City may suspend all or any portion of Contractor's performance under this Contract at its sole option and for its convenience for a reasonable period of time not to exceed six (6) months. City must first give ten (10) days' written notice to Contractor of such suspension. City will pay to Contractor a sum equivalent to the reasonable value of the goods and/or services satisfactorily provided up to the date of suspension. City may rescind the suspension prior to or at six (6) months by providing Contractor with written notice of the rescission, at which time Contractor would be required to resume performance in compliance with the terms and provisions of this Contract. Contractor will be entitled to an extension of time to complete performance under the Contract equal to the length of the suspension unless otherwise agreed to in writing by the Parties.

4.2 City's Right to Terminate for Convenience. City may, at its sole option and for its convenience, terminate all or any portion of this Contract by giving thirty (30) days' written notice of such termination to Contractor. The termination of the Contract shall be effective upon receipt of the notice by Contractor. After termination of all or any portion of the Contract, Contractor shall: (1) immediately discontinue all affected performance (unless the notice directs otherwise); and (2) complete any and all additional work necessary for the orderly filing of

documents and closing of Contractor's affected performance under the Contract. After filing of documents and completion of performance, Contractor shall deliver to City all data, drawings, specifications, reports, estimates, summaries, and such other information and materials created or received by Contractor in performing this Contract, whether completed or in process. By accepting payment for completion, filing, and delivering documents as called for in this section, Contractor discharges City of all of City's payment obligations and liabilities under this Contract with regard to the affected performance.

4.3 City's Right to Terminate for Default. Contractor's failure to satisfactorily perform any obligation required by this Contract constitutes a default. Examples of default include a determination by City that Contractor has: (1) failed to deliver goods and/or perform the services of the required quality or within the time specified; (2) failed to perform any of the obligations of this Contract; and (3) failed to make sufficient progress in performance which may jeopardize full performance.

4.3.1 If Contractor fails to satisfactorily cure a default within ten (10) calendar days of receiving written notice from City specifying the nature of the default, City may immediately cancel and/or terminate this Contract, and terminate each and every right of Contractor, and any person claiming any rights by or through Contractor under this Contract.

4.3.2 If City terminates this Contract, in whole or in part, City may procure, upon such terms and in such manner as the Purchasing Agent may deem appropriate, equivalent goods or services and Contractor shall be liable to City for any excess costs. Contractor shall also continue performance to the extent not terminated.

4.4 Termination for Bankruptcy or Assignment for the Benefit of Creditors. If Contractor files a voluntary petition in bankruptcy, is adjudicated bankrupt, or makes a general assignment for the benefit of creditors, the City may at its option and without further notice to, or demand upon Contractor, terminate this Contract, and terminate each and every right of Contractor, and any person claiming rights by and through Contractor under this Contract.

4.5 Contractor's Right to Payment Following Contract Termination.

4.5.1 Termination for Convenience. If the termination is for the convenience of City an equitable adjustment in the Contract price shall be made. No amount shall be allowed for anticipated profit on unperformed services, and no amount shall be paid for an as needed contract beyond the Contract termination date.

4.5.2 Termination for Default. If, after City gives notice of termination for failure to fulfill Contract obligations to Contractor, it is determined that Contractor had not so failed, the termination shall be deemed to have been effected for the convenience of City. In such event, adjustment in the Contract price shall be made as provided in Section 4.3.2. City's rights and remedies are in addition to any other rights and remedies provided by law or under this Contract.

4.6 Remedies Cumulative. City's remedies are cumulative and are not intended to be exclusive of any other remedies or means of redress to which City may be lawfully entitled in case of any breach or threatened breach of any provision of this Contract.

ARTICLE V
ADDITIONAL CONTRACTOR OBLIGATIONS

5.1 Inspection and Acceptance. The City will inspect and accept goods provided under this Contract at the shipment destination unless specified otherwise. Inspection will be made and acceptance will be determined by the City department shown in the shipping address of the Purchase Order or other duly authorized representative of City.

5.2 Responsibility for Lost or Damaged Shipments. Contractor bears the risk of loss or damage to goods prior to the time of their receipt and acceptance by City. City has no obligation to accept damaged shipments and reserves the right to return damaged goods, at Contractor's sole expense, even if the damage was not apparent or discovered until after receipt.

5.3 Responsibility for Damages. Contractor is responsible for all damage that occurs as a result of Contractor's fault or negligence or that of its' employees, agents, or representatives in connection with the performance of this Contract. Contractor shall immediately report any such damage to people and/or property to the Contract Administrator.

5.4 Delivery. Delivery shall be made on the delivery day specified in the Contract Documents. The City, in its sole discretion, may extend the time for delivery. The City may order, in writing, the suspension, delay or interruption of delivery of goods and/or services.

5.5 Delay. Unless otherwise specified herein, time is of the essence for each and every provision of the Contract. Contractor must immediately notify City in writing if there is, or it is anticipated that there will be, a delay in performance. The written notice must explain the cause for the delay and provide a reasonable estimate of the length of the delay. City may terminate this Contract as provided herein if City, in its sole discretion, determines the delay is material.

5.5.1 If a delay in performance is caused by any unforeseen event(s) beyond the control of the parties, City may allow Contractor to a reasonable extension of time to complete performance, but Contractor will not be entitled to damages or additional compensation. Any such extension of time must be approved in writing by City. The following conditions may constitute such a delay: war; changes in law or government regulation; labor disputes; strikes; fires, floods, adverse weather or other similar condition of the elements necessitating cessation of the performance; inability to obtain materials, equipment or labor; or other specific reasons agreed to between City and Contractor. This provision does not apply to a delay caused by Contractor's acts or omissions. Contractor is not entitled to an extension of time to perform if a delay is caused by Contractor's inability to obtain materials, equipment, or labor unless City has received, in a timely manner, documentary proof satisfactory to City of Contractor's inability to obtain materials, equipment, or labor, in which case City's approval must be in writing.

5.6 Restrictions and Regulations Requiring Contract Modification. Contractor shall immediately notify City in writing of any regulations or restrictions that may or will require Contractor to alter the material, quality, workmanship, or performance of the goods and/or services to be provided. City reserves the right to accept any such alteration, including any resulting reasonable price adjustments, or to cancel the Contract at no expense to the City.

5.7 Warranties. All goods and/or services provided under the Contract must be warranted by Contractor or manufacturer for at least twelve (12) months after acceptance by City, except automotive equipment. Automotive equipment must be warranted for a minimum of 12,000 miles or 12 months, whichever occurs first, unless otherwise stated in the Contract. Contractor is responsible to City for all warranty service, parts, and labor. Contractor is required to ensure that warranty work is performed at a facility acceptable to City and that services, parts, and labor are available and provided to meet City's schedules and deadlines. Contractor may establish a warranty service contract with an agency satisfactory to City instead of performing the warranty service itself. If Contractor is not an authorized service center and causes any damage to equipment being serviced, which results in the existing warranty being voided, Contractor will be liable for all costs of repairs to the equipment, or the costs of replacing the equipment with new equipment that meets City's operational needs.

5.8 Industry Standards. Contractor shall provide goods and/or services acceptable to City in strict conformance with the Contract. Contractor shall also provide goods and/or services in accordance with the standards customarily adhered to by an experienced and competent provider of the goods and/or services called for under this Contract using the degree of care and skill ordinarily exercised by reputable providers of such goods and/or services. Where approval by City, the Mayor, or other representative of City is required, it is understood to be general approval only and does not relieve Contractor of responsibility for complying with all applicable laws, codes, policies, regulations, and good business practices.

5.9 Records Retention and Examination. Contractor shall retain, protect, and maintain in an accessible location all records and documents, including paper, electronic, and computer records, relating to this Contract for five (5) years after receipt of final payment by City under this Contract. Contractor shall make all such records and documents available for inspection, copying, or other reproduction, and auditing by authorized representatives of City, including the Purchasing Agent or designee. Contractor shall make available all requested data and records at reasonable locations within City or County of San Diego at any time during normal business hours, and as often as City deems necessary. If records are not made available within the City or County of San Diego, Contractor shall pay City's travel costs to the location where the records are maintained and shall pay for all related travel expenses. Failure to make requested records available for inspection, copying, or other reproduction, or auditing by the date requested may result in termination of the Contract. Contractor must include this provision in all subcontracts made in connection with this Contract.

5.9.1 Contractor shall maintain records of all subcontracts entered into with all firms, all project invoices received from Subcontractors and Suppliers, all purchases of materials and services from Suppliers, and all joint venture participation. Records shall show name, telephone number including area code, and business address of each Subcontractor and Supplier, and joint venture partner, and the total amount actually paid to each firm. Project relevant records, regardless of tier, may be periodically reviewed by the City.

5.10 Quality Assurance Meetings. Upon City's request, Contractor shall schedule one or more quality assurance meetings with City's Contract Administrator to discuss Contractor's performance. If requested, Contractor shall schedule the first quality assurance meeting no later than eight (8) weeks from the date of commencement of work under the Contract. At the quality assurance meeting(s), City's Contract Administrator will provide Contractor with feedback, will note any deficiencies in Contract performance, and provide Contractor with an opportunity to address and correct such deficiencies. The total number of quality assurance meetings that may be required by City will depend upon Contractor's performance.

5.11 Duty to Cooperate with Auditor. The City Auditor may, in his sole discretion, at no cost to the City, and for purposes of performing his responsibilities under Charter section 39.2, review Contractor's records to confirm contract compliance. Contractor shall make reasonable efforts to cooperate with Auditor's requests.

5.12 Safety Data Sheets. If specified by City in the solicitation or otherwise required by this Contract, Contractor must send with each shipment one (1) copy of the Safety Data Sheet (SDS) for each item shipped. Failure to comply with this procedure will be cause for immediate termination of the Contract for violation of safety procedures.

5.13 Project Personnel. Except as formally approved by the City, the key personnel identified in Contractor's bid or proposal shall be the individuals who will actually complete the work. Changes in staffing must be reported in writing and approved by the City.

5.13.1 Criminal Background Certification. Contractor certifies that all employees working on this Contract have had a criminal background check and that said employees are clear of any sexual and drug related convictions. Contractor further certifies that all employees hired by Contractor or a subcontractor shall be free from any felony convictions.

5.13.2 Photo Identification Badge. Contractor shall provide a company photo identification badge to any individual assigned by Contractor or subcontractor to perform services or deliver goods on City premises. Such badge must be worn at all times while on City premises. City reserves the right to require Contractor to pay fingerprinting fees for personnel assigned to work in sensitive areas. All employees shall turn in their photo identification badges to Contractor upon completion of services and prior to final payment of invoice.

5.14 Standards of Conduct. Contractor is responsible for maintaining standards of employee competence, conduct, courtesy, appearance, honesty, and integrity satisfactory to the City.

5.14.1 Supervision. Contractor shall provide adequate and competent supervision at all times during the Contract term. Contractor shall be readily available to meet with the City. Contractor shall provide the telephone numbers where its representative(s) can be reached.

5.14.2 City Premises. Contractor's employees and agents shall comply with all City rules and regulations while on City premises.

5.14.3 Removal of Employees. City may request Contractor immediately remove from assignment to the City any employee found unfit to perform duties at the City. Contractor shall comply with all such requests.

5.15 Licenses and Permits. Contractor shall, without additional expense to the City, be responsible for obtaining any necessary licenses, permits, certifications, accreditations, fees and approvals for complying with any federal, state, county, municipal, and other laws, codes, and regulations applicable to Contract performance. This includes, but is not limited to, any laws or regulations requiring the use of licensed contractors to perform parts of the work.

5.16 Contractor and Subcontractor Registration Requirements. Prior to the award of the Contract or Task Order, Contractor and Contractor's subcontractors and suppliers must register with the City's web-based vendor registration and bid management system. The City may not award the Contract until registration of all subcontractors and suppliers is complete. In the event this requirement is not met within the time frame specified by the City, the City reserves the right to rescind the Contract award and to make the award to the next responsive and responsible proposer of bidder.

ARTICLE VI
INTELLECTUAL PROPERTY RIGHTS

6.1 Rights in Data. If, in connection with the services performed under this Contract, Contractor or its employees, agents, or subcontractors, create artwork, audio recordings, blueprints, designs, diagrams, documentation, photographs, plans, reports, software, source code, specifications, surveys, system designs, video recordings, or any other original works of authorship, whether written or readable by machine (Deliverable Materials), all rights of Contractor or its subcontractors in the Deliverable Materials, including, but not limited to publication, and registration of copyrights, and trademarks in the Deliverable Materials, are the sole property of City. Contractor, including its employees, agents, and subcontractors, may not use any Deliverable Material for purposes unrelated to Contractor's work on behalf of the City without prior written consent of City. Contractor may not publish or reproduce any Deliverable Materials, for purposes unrelated to Contractor's work on behalf of the City, without the prior written consent of the City.

6. 2 Intellectual Property Rights Assignment. For no additional compensation, Contractor hereby assigns to City all of Contractor's rights, title, and interest in and to the content of the Deliverable Materials created by Contractor or its employees, agents, or subcontractors, including copyrights, in connection with the services performed under this Contract. Contractor

shall promptly execute and deliver, and shall cause its employees, agents, and subcontractors to promptly execute and deliver, upon request by the City or any of its successors or assigns at any time and without further compensation of any kind, any power of attorney, assignment, application for copyright, patent, trademark or other intellectual property right protection, or other papers or instruments which may be necessary or desirable to fully secure, perfect or otherwise protect to or for the City, its successors and assigns, all right, title and interest in and to the content of the Deliverable Materials. Contractor also shall cooperate and assist in the prosecution of any action or opposition proceeding involving such intellectual property rights and any adjudication of those rights.

6. 3 Contractor Works. Contractor Works means tangible and intangible information and material that: (a) had already been conceived, invented, created, developed or acquired by Contractor prior to the effective date of this Contract; or (b) were conceived, invented, created, or developed by Contractor after the effective date of this Contract, but only to the extent such information and material do not constitute part or all of the Deliverable Materials called for in this Contract. All Contractor Works, and all modifications or derivatives of such Contractor Works, including all intellectual property rights in or pertaining to the same, shall be owned solely and exclusively by Contractor.

6. 4 Subcontracting. In the event that Contractor utilizes a subcontractor(s) for any portion of the work that comprises the whole or part of the specified Deliverable Materials to the City, the agreement between Contractor and the subcontractor shall include a statement that identifies the Deliverable Materials as a "works for hire" as described in the United States Copyright Act of 1976, as amended, and that all intellectual property rights in the Deliverable Materials, whether arising in copyright, trademark, service mark or other forms of intellectual property rights, belong to and shall vest solely with the City. Further, the agreement between Contractor and its subcontractor shall require that the subcontractor, if necessary, shall grant, transfer, sell and assign, free of charge, exclusively to City, all titles, rights and interests in and to the Deliverable Materials, including all copyrights, trademarks and other intellectual property rights. City shall have the right to review any such agreement for compliance with this provision.

6. 5 Intellectual Property Warranty and Indemnification. Contractor represents and warrants that any materials or deliverables, including all Deliverable Materials, provided under this Contract are either original, or not encumbered, and do not infringe upon the copyright, trademark, patent or other intellectual property rights of any third party, or are in the public domain. If Deliverable Materials provided hereunder become the subject of a claim, suit or allegation of copyright, trademark or patent infringement, City shall have the right, in its sole discretion, to require Contractor to produce, at Contractor's own expense, new non-infringing materials, deliverables or works as a means of remedying any claim of infringement in addition to any other remedy available to the City under law or equity. Contractor further agrees to indemnify, defend, and hold harmless the City, its officers, employees and agents from and against any and all claims, actions, costs, judgments or damages, of any type, alleging or threatening that any Deliverable Materials, supplies, equipment, services or works provided under this contract infringe the copyright, trademark, patent or other intellectual property or proprietary rights of any third party (Third Party Claim of Infringement). If a Third Party Claim

of Infringement is threatened or made before Contractor receives payment under this Contract, City shall be entitled, upon written notice to Contractor, to withhold some or all of such payment.

6.6 Software Licensing. Contractor represents and warrants that the software, if any, as delivered to City, does not contain any program code, virus, worm, trap door, back door, time or clock that would erase data or programming or otherwise cause the software to become inoperable, inaccessible, or incapable of being used in accordance with its user manuals, either automatically, upon the occurrence of licensor-selected conditions or manually on command. Contractor further represents and warrants that all third party software, delivered to City or used by Contractor in the performance of the Contract, is fully licensed by the appropriate licensor.

6.7 Publication. Contractor may not publish or reproduce any Deliverable Materials, for purposes unrelated to Contractor's work on behalf of the City without prior written consent from the City.

6.8 Royalties, Licenses, and Patents. Unless otherwise specified, Contractor shall pay all royalties, license, and patent fees associated with the goods that are the subject of this solicitation. Contractor warrants that the goods, materials, supplies, and equipment to be supplied do not infringe upon any patent, trademark, or copyright, and further agrees to defend any and all suits, actions and claims for infringement that are brought against the City, and to defend, indemnify and hold harmless the City, its elected officials, officers, and employees from all liability, loss and damages, whether general, exemplary or punitive, suffered as a result of any actual or claimed infringement asserted against the City, Contractor, or those furnishing goods, materials, supplies, or equipment to Contractor under the Contract.

ARTICLE VII
INDEMNIFICATION AND INSURANCE

7.1 Indemnification. To the fullest extent permitted by law, Contractor shall defend (with legal counsel reasonably acceptable to City), indemnify, protect, and hold harmless City and its elected officials, officers, employees, agents, and representatives (Indemnified Parties) from and against any and all claims, losses, costs, damages, injuries (including, without limitation, injury to or death of an employee of Contractor or its subcontractors), expense, and liability of every kind, nature and description (including, without limitation, incidental and consequential damages, court costs, and litigation expenses and fees of expert consultants or expert witnesses incurred in connection therewith and costs of investigation) that arise out of, pertain to, or relate to, directly or indirectly, in whole or in part, any goods provided or performance of services under this Contract by Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or anyone that either of them control. Contractor's duty to defend, indemnify, protect and hold harmless shall not include any claims or liabilities arising from the sole negligence or willful misconduct of the Indemnified Parties.

7.2 Insurance. Contractor shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or

in connection with the performance of the work hereunder and the results of that work by Contractor, his agents, representatives, employees or subcontractors.

Contractor shall provide, at a minimum, the following:

7.2.1 Commercial General Liability. Insurance Services Office Form CG 00 01 covering CGL on an "occurrence" basis, including products and completed operations, property damage, bodily injury, and personal and advertising injury with limits no less than $1,000,000 per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location (ISO CG 25 03 or 25 04) or the general aggregate limit shall be twice the required occurrence limit.

7.2.2 Commercial Automobile Liability. Insurance Services Office Form Number CA 0001 covering Code 1 (any auto) or, if Contractor has no owned autos, Code 8 (hired) and 9 (non-owned), with limit no less than $1,000,000 per accident for bodily injury and property damage.

7.2.3 Workers' Compensation. Insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than $1,000,000 per accident for bodily injury or disease.

7.2.4 Professional Liability (Errors and Omissions). For consultant contracts, insurance appropriate to Consultant's profession, with limit no less than $1,000,000 per occurrence or claim, $2,000,000 aggregate.

If Contractor maintains broader coverage and/or higher limits than the minimums shown above, City requires and shall be entitled to the broader coverage and/or the higher limits maintained by Contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to City.

7.2.5 Other Insurance Provisions. The insurance policies are to contain, or be endorsed to contain, the following provisions:

7.2.5.1 Additional Insured Status. The City, its officers, officials, employees, and volunteers are to be covered as additional insureds on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of Contractor including materials, parts, or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to Contractor's insurance (at least as broad as ISO Form CG 20 10 11 85 or if not available, through the addition of both CG 20 10, CG 20 26, CG 20 33, or CG 20 38; and CG 20 37 if a later edition is used).

7.2.5.2 Primary Coverage. For any claims related to this contract, Contractor's insurance coverage shall be primary coverage at least as broad as ISO CG 20 01 04 13 as respects the City, its officers, officials, employees, and volunteers. Any insurance or self-insurance maintained by City, its officers, officials, employees, or volunteers shall be excess of Contractor's insurance and shall not contribute with it.

7.2.5.3 Notice of Cancellation. Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to City.

7.2.5.4 Waiver of Subrogation. Contractor hereby grants to City a waiver of any right to subrogation which the Workers' Compensation insurer of said Contractor may acquire against City by virtue of the payment of any loss under such insurance. Contractor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the City has received a waiver of subrogation endorsement from the insurer.

7.2.5.5 Claims Made Policies (applicable only to professional liability). The Retroactive Date must be shown, and must be before the date of the contract or the beginning of contract work. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the contract of work. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, Contractor must purchase "extended reporting" coverage for a minimum of five (5) years after completion of work.

7.3 Self Insured Retentions. Self-insured retentions must be declared to and approved by City. City may require Contractor to purchase coverage with a lower retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. The policy language shall provide, or be endorsed to provide, that the self-insured retention may be satisfied by either the named insured or City.

7.4 Acceptability of Insurers. Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A-VI, unless otherwise acceptable to City.

City will accept insurance provided by non-admitted, "surplus lines" carriers only if the carrier is authorized to do business in the State of California and is included on the List of Approved Surplus Lines Insurers (LASLI list). All policies of insurance carried by non-admitted carriers are subject to all of the requirements for policies of insurance provided by admitted carriers described herein.

7.5 Verification of Coverage. Contractor shall furnish City with original certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this clause. All certificates and endorsements are to be received and approved by City before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive Contractor's obligation to provide them. City reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.

7.6 Special Risks or Circumstances. City reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

7.7 Additional Insurance. Contractor may obtain additional insurance not required by this Contract.

7.8 Excess Insurance. All policies providing excess coverage to City shall follow the form of the primary policy or policies including but not limited to all endorsements.

7.9 Subcontractors. Contractor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Contractor shall ensure that City is an additional insured on insurance required from subcontractors. For CGL coverage, subcontractors shall provide coverage with a format at least as broad as the CG 20 38 04 13 endorsement.

ARTICLE VIII
BONDS

8.1 Payment and Performance Bond. Prior to the execution of this Contract, City may require Contractor to post a payment and performance bond (Bond). The Bond shall guarantee Contractor's faithful performance of this Contract and assure payment to contractors, subcontractors, and to persons furnishing goods and/or services under this Contract.

8.1.1 Bond Amount. The Bond shall be in a sum equal to twenty-five percent (25%) of the Contract amount, unless otherwise stated in the Specifications. City may file a claim against the Bond if Contractor fails or refuses to fulfill the terms and provisions of the Contract.

8.1.2 Bond Term. The Bond shall remain in full force and effect at least until complete performance of this Contract and payment of all claims for materials and labor, at which time it will convert to a ten percent (10%) warranty bond, which shall remain in place until the end of the warranty periods set forth in this Contract. The Bond shall be renewed annually, at least sixty (60) days in advance of its expiration, and Contractor shall provide timely proof of annual renewal to City.

8.1.3 Bond Surety. The Bond must be furnished by a company authorized by the State of California Department of Insurance to transact surety business in the State of California and which has a current A.M. Best rating of at least "A-, VIII."

8.1.4 Non-Renewal or Cancellation. The Bond must provide that City and Contractor shall be provided with sixty (60) days' advance written notice in the event of non-renewal, cancellation, or material change to its terms. In the event of non-renewal, cancellation, or material change to the Bond terms, Contractor shall provide City with evidence of the new source of surety within twenty-one (21) calendar days after the date of the notice of non-renewal, cancellation, or material change. Failure to maintain the Bond, as required herein, in full force

and effect as required under this Contact, will be a material breach of the Contract subject to termination of the Contract.

8.2 Alternate Security. City may, at its sole discretion, accept alternate security in the form of an endorsed certificate of deposit, a money order, a certified check drawn on a solvent bank, or other security acceptable to the Purchasing Agent in an amount equal to the required Bond.

ARTICLE IX
CITY-MANDATED CLAUSES AND REQUIREMENTS

9.1 Contractor Certification of Compliance. By signing this Contract, Contractor certifies that Contractor is aware of, and will comply with, these City-mandated clauses throughout the duration of the Contract.

9.1.1 Drug-Free Workplace Certification. Contractor shall comply with City's Drug-Free Workplace requirements set forth in Council Policy 100-17, which is incorporated into the Contract by this reference.

9.1.2 Contractor Certification for Americans with Disabilities Act (ADA) and State Access Laws and Regulations: Contractor shall comply with all accessibility requirements under the ADA and under Title 24 of the California Code of Regulations (Title 24). When a conflict exists between the ADA and Title 24, Contractor shall comply with the most restrictive requirement (i.e., that which provides the most access). Contractor also shall comply with the City's ADA Compliance/City Contractors requirements as set forth in Council Policy 100-04, which is incorporated into this Contract by reference. Contractor warrants and certifies compliance with all federal and state access laws and regulations and further certifies that any subcontract agreement for this contract contains language which indicates the subcontractor's agreement to abide by the provisions of the City's Council Policy and any applicable access laws and regulations.

9.1.3 Non-Discrimination Requirements.

9.1.3.1 Compliance with City's Equal Opportunity Contracting Program (EOCP). Contractor shall comply with City's EOCP Requirements. Contractor shall not discriminate against any employee or applicant for employment on any basis prohibited by law. Contractor shall provide equal opportunity in all employment practices. Prime Contractors shall ensure that their subcontractors comply with this program. Nothing in this Section shall be interpreted to hold a Prime Contractor liable for any discriminatory practice of its subcontractors.

9.1.3.2 Non-Discrimination Ordinance. Contractor shall not discriminate on the basis of race, gender, gender expression, gender identity, religion, national origin, ethnicity, sexual orientation, age, or disability in the solicitation, selection, hiring or treatment of subcontractors, vendors or suppliers. Contractor shall provide equal opportunity for subcontractors to participate in subcontracting opportunities. Contractor understands and agrees that violation of this clause shall be considered a material breach of the Contract and may result

in Contract termination, debarment, or other sanctions. Contractor shall ensure that this language is included in contracts between Contractor and any subcontractors, vendors and suppliers.

9.1.3.3 Compliance Investigations. Upon City's request, Contractor agrees to provide to City, within sixty calendar days, a truthful and complete list of the names of all subcontractors, vendors, and suppliers that Contractor has used in the past five years on any of its contracts that were undertaken within San Diego County, including the total dollar amount paid by Contractor for each subcontract or supply contract. Contractor further agrees to fully cooperate in any investigation conducted by City pursuant to City's Nondiscrimination in Contracting Ordinance. Contractor understands and agrees that violation of this clause shall be considered a material breach of the Contract and may result in Contract termination, debarment, and other sanctions.

9.1.4 Equal Benefits Ordinance Certification. Unless an exception applies, Contractor shall comply with the Equal Benefits Ordinance (EBO) codified in the San Diego Municipal Code (SDMC). Failure to maintain equal benefits is a material breach of the Contract.

9.1.5 Contractor Standards. Contractor shall comply with Contractor Standards provisions codified in the SDMC. Contractor understands and agrees that violation of Contractor Standards may be considered a material breach of the Contract and may result in Contract termination, debarment, and other sanctions.

9.1.6 Noise Abatement. Contractor shall operate, conduct, or construct without violating the City's Noise Abatement Ordinance codified in the SDMC.

9.1.7 Storm Water Pollution Prevention Program. Contractor shall comply with the City's Storm Water Management and Discharge Control provisions codified in Division 3 of Chapter 4 of the SDMC, as may be amended, and any and all applicable Best Management Practice guidelines and pollution elimination requirements in performing or delivering services at City owned, leased, or managed property, or in performance of services and activities on behalf of City regardless of location.

Contractor shall comply with the City's Jurisdictional Urban Runoff Management Plan encompassing Citywide programs and activities designed to prevent and reduce storm water pollution within City boundaries as adopted by the City Council on January 22, 2008, via Resolution No. 303351, as may be amended.

Contractor shall comply with each City facility or work site's Storm Water Pollution Prevention Plan, as applicable, and institute all controls needed while completing the services to minimize any negative impact to the storm water collection system and environment.

9.1.8 Service Worker Retention Ordinance. If applicable, Contractor shall comply with the Service Worker Retention Ordinance (SWRO) codified in the SDMC.

9.1.9 Product Endorsement. Contractor shall comply with Council Policy 000-41 which requires that other than listing the City as a client and other limited endorsements, any advertisements, social media, promotions or other marketing referring to the City as a user of a product or service will require prior written approval of the Mayor or designee. Use of the City Seal or City logos is prohibited.

9.1.10 Business Tax Certificate. Unless the City Treasurer determines in writing that a contractor is exempt from the payment of business tax, any contractor doing business with the City of San Diego is required to obtain a Business Tax Certificate (BTC) and to provide a copy of its BTC to the City before a Contract is executed.

9.1.11 Equal Pay Ordinance. Unless an exception applies, Contractor shall comply with the Equal Pay Ordinance codified in San Diego Municipal Code sections 22.4801 through 22.4809. Contractor shall certify in writing that it will comply with the requirements of the EPO.

9.1.11.1 Contractor and Subcontract Requirement. The Equal Pay Ordinance applies to any subcontractor who performs work on behalf of a Contractor to the same extent as it would apply to that Contractor. Any Contractor subject to the Equal Pay Ordinance shall require all of its subcontractors to certify compliance with the Equal Pay Ordinance in its written subcontracts.

ARTICLE X
CONFLICT OF INTEREST AND VIOLATIONS OF LAW

10.1 Conflict of Interest Laws. Contractor is subject to all federal, state and local conflict of interest laws, regulations, and policies applicable to public contracts and procurement practices including, but not limited to, California Government Code sections 1090, *et. seq.* and 81000*, et. seq.,* and the Ethics Ordinance, codified in the SDMC. City may determine that Contractor must complete one or more statements of economic interest disclosing relevant financial interests. Upon City's request, Contractor shall submit the necessary documents to City.

10.2 Contractor's Responsibility for Employees and Agents. Contractor is required to establish and make known to its employees and agents appropriate safeguards to prohibit employees from using their positions for a purpose that is, or that gives the appearance of being, motivated by the desire for private gain for themselves or others, particularly those with whom they have family, business or other relationships.

10.3 Contractor's Financial or Organizational Interests. In connection with any task, Contractor shall not recommend or specify any product, supplier, or contractor with whom Contractor has a direct or indirect financial or organizational interest or relationship that would violate conflict of interest laws, regulations, or policies.

10.4 Certification of Non-Collusion. Contractor certifies that: (1) Contractor's bid or proposal was not made in the interest of or on behalf of any person, firm, or corporation not identified; (2) Contractor did not directly or indirectly induce or solicit any other bidder or proposer to put in a sham bid or proposal; (3) Contractor did not directly or indirectly induce or

solicit any other person, firm or corporation to refrain from bidding; and (4) Contractor did not seek by collusion to secure any advantage over the other bidders or proposers.

10.5 Hiring City Employees. This Contract shall be unilaterally and immediately terminated by City if Contractor employs an individual who within the twelve (12) months immediately preceding such employment did in his/her capacity as a City officer or employee participate in negotiations with or otherwise have an influence on the selection of Contractor.

ARTICLE XI
DISPUTE RESOLUTION

11.1 Mediation. If a dispute arises out of or relates to this Contract and cannot be settled through normal contract negotiations, Contractor and City shall use mandatory non-binding mediation before having recourse in a court of law.

11.2 Selection of Mediator. A single mediator that is acceptable to both parties shall be used to mediate the dispute. The mediator will be knowledgeable in the subject matter of this Contract, if possible.

11.3 Expenses. The expenses of witnesses for either side shall be paid by the party producing such witnesses. All other expenses of the mediation, including required traveling and other expenses of the mediator, and the cost of any proofs or expert advice produced at the direct request of the mediator, shall be borne equally by the parties, unless they agree otherwise.

11.4 Conduct of Mediation Sessions. Mediation hearings will be conducted in an informal manner and discovery will not be allowed. The discussions, statements, writings and admissions will be confidential to the proceedings (pursuant to California Evidence Code sections 1115 through 1128) and will not be used for any other purpose unless otherwise agreed by the parties in writing. The parties may agree to exchange any information they deem necessary. Both parties shall have a representative attend the mediation who is authorized to settle the dispute, though City's recommendation of settlement may be subject to the approval of the Mayor and City Council. Either party may have attorneys, witnesses or experts present.

11.5 Mediation Results. Any agreements resulting from mediation shall be memorialized in writing. The results of the mediation shall not be final or binding unless otherwise agreed to in writing by the parties. Mediators shall not be subject to any subpoena or liability, and their actions shall not be subject to discovery.

ARTICLE XII
MANDATORY ASSISTANCE

12.1 Mandatory Assistance. If a third party dispute or litigation, or both, arises out of, or relates in any way to the services provided to the City under a Contract, Contractor , its agents, officers, and employees agree to assist in resolving the dispute or litigation upon City’s request. Contractor’s assistance includes, but is not limited to, providing professional consultations,

attending mediations, arbitrations, depositions, trials or any event related to the dispute resolution and/or litigation.

12.2 Compensation for Mandatory Assistance. City will compensate Contractor for fees incurred for providing Mandatory Assistance. If, however, the fees incurred for the Mandatory Assistance are determined, through resolution of the third party dispute or litigation, or both, to be attributable in whole, or in part, to the acts or omissions of Contractor, its agents, officers, and employees, Contractor shall reimburse City for all fees paid to Contractor, its agents, officers, and employees for Mandatory Assistance.

12.3 Attorneys' Fees Related to Mandatory Assistance. In providing City with dispute or litigation assistance, Contractor or its agents, officers, and employees may incur expenses and/or costs. Contractor agrees that any attorney fees it may incur as a result of assistance provided under Section 12.2 are not reimbursable.

ARTICLE XIII
MISCELLANEOUS

13.1 Headings. All headings are for convenience only and shall not affect the interpretation of this Contract.

13.2 Non-Assignment. Contractor may not assign the obligations under this Contract, whether by express assignment or by sale of the company, nor any monies due or to become due under this Contract, without City's prior written approval. Any assignment in violation of this paragraph shall constitute a default and is grounds for termination of this Contract at the City's sole discretion. In no event shall any putative assignment create a contractual relationship between City and any putative assignee.

13.3 Independent Contractors. Contractor and any subcontractors employed by Contractor are independent contractors and not agents of City. Any provisions of this Contract that may appear to give City any right to direct Contractor concerning the details of performing or providing the goods and/or services, or to exercise any control over performance of the Contract, shall mean only that Contractor shall follow the direction of City concerning the end results of the performance.

13.4 Subcontractors. All persons assigned to perform any work related to this Contract, including any subcontractors, are deemed to be employees of Contractor, and Contractor shall be directly responsible for their work.

13.5 Covenants and Conditions. All provisions of this Contract expressed as either covenants or conditions on the part of City or Contractor shall be deemed to be both covenants and conditions.

13.6 Compliance with Controlling Law. Contractor shall comply with all applicable local, state, and federal laws, regulations, and policies. Contractor's act or omission in violation of applicable local, state, and federal laws, regulations, and policies is grounds for contract

termination. In addition to all other remedies or damages allowed by law, Contractor is liable to City for all damages, including costs for substitute performance, sustained as a result of the violation. In addition, Contractor may be subject to suspension, debarment, or both.

13.7 Governing Law. The Contract shall be deemed to be made under, construed in accordance with, and governed by the laws of the State of California without regard to the conflicts or choice of law provisions thereof.

13.8 Venue. The venue for any suit concerning solicitations or the Contract, the interpretation of application of any of its terms and conditions, or any related disputes shall be in the County of San Diego, State of California.

13.9 Successors in Interest. This Contract and all rights and obligations created by this Contract shall be in force and effect whether or not any parties to the Contract have been succeeded by another entity, and all rights and obligations created by this Contract shall be vested and binding on any party's successor in interest.

13.10 No Waiver. No failure of either City or Contractor to insist upon the strict performance by the other of any covenant, term or condition of this Contract, nor any failure to exercise any right or remedy consequent upon a breach of any covenant, term, or condition of this Contract, shall constitute a waiver of any such breach of such covenant, term or condition. No waiver of any breach shall affect or alter this Contract, and each and every covenant, condition, and term hereof shall continue in full force and effect without respect to any existing or subsequent breach.

13.11 Severability. The unenforceability, invalidity, or illegality of any provision of this Contract shall not render any other provision of this Contract unenforceable, invalid, or illegal.

13.12 Drafting Ambiguities. The parties acknowledge that they have the right to be advised by legal counsel with respect to the negotiations, terms and conditions of this Contract, and the decision of whether to seek advice of legal counsel with respect to this Contract is the sole responsibility of each party. This Contract shall not be construed in favor of or against either party by reason of the extent to which each party participated in the drafting of the Contract.

13.13 Amendments. Neither this Contract nor any provision hereof may be changed, modified, amended or waived except by a written agreement executed by duly authorized representatives of City and Contractor. Any alleged oral amendments have no force or effect. The Purchasing Agent must sign all Contract amendments.

13.14 Conflicts Between Terms. If this Contract conflicts with an applicable local, state, or federal law, regulation, or court order, applicable local, state, or federal law, regulation, or court order shall control. Varying degrees of stringency among the main body of this Contract, the exhibits or attachments, and laws, regulations, or orders are not deemed conflicts, and the most stringent requirement shall control. Each party shall notify the other immediately upon the identification of any apparent conflict or inconsistency concerning this Contract.

13.15 Survival of Obligations. All representations, indemnifications, warranties, and guarantees made in, required by, or given in accordance with this Contract, as well as all continuing obligations indicated in this Contract, shall survive, completion and acceptance of performance and termination, expiration or completion of the Contract.

13.16 Confidentiality of Services. All services performed by Contractor, and any sub-contractor(s) if applicable, including but not limited to all drafts, data, information, correspondence, proposals, reports of any nature, estimates compiled or composed by Contractor, are for the sole use of City, its agents, and employees. Neither the documents nor their contents shall be released by Contractor or any subcontractor to any third party without the prior written consent of City. This provision does not apply to information that: (1) was publicly known, or otherwise known to Contractor, at the time it was disclosed to Contractor by City; (2) subsequently becomes publicly known through no act or omission of Contractor; or (3) otherwise becomes known to Contractor other than through disclosure by City.

13.17 Insolvency. If Contractor enters into proceedings relating to bankruptcy, whether voluntary or involuntary, Contractor agrees to furnish, by certified mail or electronic commerce method authorized by the Contract, written notification of the bankruptcy to the Purchasing Agent and the Contract Administrator responsible for administering the Contract. This notification shall be furnished within five (5) days of the initiation of the proceedings relating to bankruptcy filing. This notification shall include the date on which the bankruptcy petition was filed, the identity of the court in which the bankruptcy petition was filed, and a listing of City contract numbers and contracting offices for all City contracts against which final payment has not been made. This obligation remains in effect until final payment is made under this Contract.

13.18 No Third Party Beneficiaries. Except as may be specifically set forth in this Contract, none of the provisions of this Contract are intended to benefit any third party not specifically referenced herein. No party other than City and Contractor shall have the right to enforce any of the provisions of this Contract.

13.19 Actions of City in its Governmental Capacity. Nothing in this Contract shall be interpreted as limiting the rights and obligations of City in its governmental or regulatory capacity.

Exhibit D
Axon Enterprise, Inc's
Master Service and Purchase Agreement for
Agency

This Master Services and Purchasing Agreement ("**Agreement**") is between Axon Enterprise, Inc. ("**Axon**"), and the agency listed below or, if no agency is listed below, the agency on the Quote attached hereto ("**Agency**"). This Agreement is effective as of the later of the (a) last signature date on this Agreement or (b) signature date on the Quote ("**Effective Date**"). Axon and Agency are each a "**Party**" and collectively "**Parties**". This Agreement governs Agency's purchase and use of the Axon Devices and Services detailed in the Quote Appendix ("**Quote**"). It is the intent of the Parties that this Agreement will govern all subsequent purchases by Agency for the same Axon Devices and Services in the Quote, and all such subsequent quotes accepted by Agency shall be also incorporated into this Agreement by reference as a Quote. The Parties agree as follows:

1. **Definitions**.

   1.1. "**Axon Cloud Services**" means Axon's web services for Axon Evidence, Axon Records, Axon Dispatch, and interactions between Axon Evidence and Axon Devices or Axon client software. Axon Cloud Service excludes third-party applications, hardware warranties, and my.evidence.com.

   1.2. "**Axon Device**" means all hardware provided by Axon under this Agreement. Axon-manufactured Devices are a subset of Axon Devices.

   1.3. "**Quote**" means an offer to sell and is only valid for devices and services on the offer at the specified prices. Any inconsistent or supplemental terms within Agency's purchase order in response to a Quote will be void. Orders are subject to prior credit approval. Changes in the deployment estimated ship date may change charges in the Quote. Shipping dates are estimates only. Axon is not responsible for typographical errors in any Quote by Axon, and Axon reserves the right to cancel any orders resulting from such errors.

   1.4. "**Services**" means all services provided by Axon under this Agreement, including software, Axon Cloud Services, and professional services.

2. **Term**. This Agreement begins on the Effective Date and continues until all subscriptions hereunder have expired or have been terminated ("**Term**").

   2.1. All subscriptions including Axon Evidence, Axon Fleet, Officer Safety Plans, Technology Assurance Plans, and TASER 7 or TASER 10 plans begin on the date stated in the Quote. Each subscription term ends upon completion of the subscription stated in the Quote ("**Subscription Term**").

   2.2. Upon completion of the Subscription Term, the Subscription Term will automatically renew for an additional 5 years ("**Renewal Term**"). For purchase of TASER 7 or TASER 10 as a standalone, Axon may increase pricing to its then-current list pricing for any Renewal Term. For all other purchases, Axon may increase pricing on all line items in the Quote by up to 3% at the beginning of each year of the Renewal Term. New devices and services may require additional terms. Axon will not authorize services until Axon receives a signed Quote or accepts a purchase order, whichever is first.

3. **Payment**. Axon invoices upon shipment, or on the date specified within the invoicing plan in the Quote. Payment is due net 30 days from the invoice date. Payment obligations are non-cancelable. Unless otherwise prohibited by law, Agency will pay interest on all past-due sums at the lower of one-and-a-half percent (1.5%) per month or the highest rate allowed by law. Agency will pay invoices without setoff, deduction, or withholding. If Axon sends a past due account to collections, Agency is responsible for collection and attorneys' fees.

4. **Taxes**. Agency is responsible for sales and other taxes associated with the order unless Agency provides Axon a valid tax exemption certificate.

5. **Shipping**. Axon may make partial shipments and ship Axon Devices from multiple locations. All shipments are EXW (Incoterms 2020) via common carrier. Title and risk of loss pass to Agency upon Axon's delivery to the common carrier. Agency is responsible for any shipping charges in the Quote.

6. **Returns**. All sales are final. Axon does not allow refunds or exchanges, except warranty returns or as provided by state or federal law.

7. **Warranty**.

   7.1. **Limited Warranty**. Axon warrants that Axon-manufactured Devices are free from defects in workmanship and materials for one (1) year from the date of Agency's receipt, except Signal Sidearm and Axon-manufactured accessories, which Axon warrants for thirty (30) months and ninety (90) days, respectively, from the date of Agency's receipt. Used conducted energy weapon ("**CEW**") cartridges are deemed to have operated properly. Extended warranties run from the expiration of the one- (1-) year hardware warranty through the extended warranty term.

   7.2. **Disclaimer. All software and Axon Cloud Services are provided "AS IS," without any warranty of any kind, either express or implied, including without limitation the implied warranties of merchantability,**

fitness for a particular purpose and non-infringement. Axon Devices and Services that are not manufactured, published or performed by Axon ("Third-Party Products") are not covered by Axon's warranty and are only subject to the warranties of the third-party provider or manufacturer.

7.3. **Claims**. If Axon receives a valid warranty claim for an Axon-manufactured Device during the warranty term, Axon's sole responsibility is to repair or replace the Axon-manufactured Device with the same or like Axon-manufactured Device, at Axon's option. A replacement Axon-manufactured Device will be new or like new. Axon will warrant the replacement Axon-manufactured Device for the longer of (a) the remaining warranty of the original Axon-manufactured Device or (b) ninety (90) days from the date of repair or replacement.

7.3.1. If Agency exchanges an Axon Device or part, the replacement item becomes Agency's property, and the replaced item becomes Axon's property. Before delivering an Axon-manufactured Device for service, Agency must upload Axon-manufactured Device data to Axon Evidence or download it and retain a copy. Axon is not responsible for any loss of software, data, or other information contained in storage media or any part of the Axon-manufactured Device sent to Axon for service.

7.4. **Spare Axon Devices**. At Axon's reasonable discretion, Axon may provide Agency a predetermined number of spare Axon Devices as detailed in the Quote ("**Spare Axon Devices**"). Spare Axon Devices are intended to replace broken or non-functioning units while Agency submits the broken or non-functioning units, through Axon's warranty return process. Axon will repair or replace the unit with a replacement Axon Device. Title and risk of loss for all Spare Axon Devices shall pass to Agency in accordance with shipping terms under Section 5. Axon assumes no liability or obligation in the event Agency does not utilize Spare Axon Devices for the intended purpose.

7.5. **Limitations**. Axon's warranty excludes damage related to: (a) failure to follow Axon Device use instructions; (b) Axon Devices used with equipment not manufactured or recommended by Axon; (c) abuse, misuse, or intentional damage to Axon Device; (d) force majeure; (e) Axon Devices repaired or modified by persons other than Axon without Axon's written permission; or (f) Axon Devices with a defaced or removed serial number. Axon's warranty will be void if Agency resells Axon Devices.

7.5.1. To the extent permitted by law, the above warranties and remedies are exclusive. Axon disclaims all other warranties, remedies, and conditions, whether oral, written, statutory, or implied. If statutory or implied warranties cannot be lawfully disclaimed, then such warranties are limited to the duration of the warranty described above and by the provisions in this Agreement. Agency confirms and agrees that, in deciding whether to sign this Agreement, it has not relied on any statement or representation by Axon or anyone acting on behalf of Axon related to the subject matter of this Agreement that is not in this Agreement.

7.5.2. Axon's cumulative liability to any party for any loss or damage resulting from any claim, demand, or action arising out of or relating to any Axon Device or Service will not exceed the purchase price paid to Axon for the Axon Device, or if for Services, the amount paid for such Services over the twelve (12) months preceding the claim. Neither Party will be liable for direct, special, indirect, incidental, punitive or consequential damages, however caused, whether for breach of warranty or contract, negligence, strict liability, tort or any other legal theory.

7.6. **Online Support Platforms**. Use of Axon's online support platforms (e.g., Axon Academy and MyAxon) is governed by the Axon Online Support Platforms Terms of Use Appendix available at www.axon.com/sales-terms-and-conditions.

7.7. **Third-Party Software and Services**. Use of software or services other than those provided by Axon is governed by the terms, if any, entered into between Agency and the respective third-party provider, including, without limitation, the terms applicable to such software or services located at www.axon.com/sales-terms-and-conditions, if any.

7.8. **Axon Aid**. Upon mutual agreement between Axon and Agency, Axon may provide certain products and services to Agency, as a charitable donation under the Axon Aid program. In such event, Agency expressly waives and releases any and all claims, now known or hereafter known, against Axon and its officers, directors, employees, agents, contractors, affiliates, successors, and assigns (collectively, "**Releasees**"), including but not limited to, on account of injury, death, property damage, or loss of data, arising out of or attributable to the Axon Aid program whether arising out of the negligence of any Releasees or otherwise. Agency agrees not to make or bring any such claim against any Releasee, and forever release and discharge all Releasees from liability under such claims. Agency expressly allows Axon to publicly announce its participation in Axon Aid and use its name in marketing materials. Axon may terminate the Axon Aid program without cause immediately upon notice to the Agency.

8. **Statement of Work**. Certain Axon Devices and Services, including Axon Interview Room, Axon Channel Services,

and Axon Fleet, may require a Statement of Work that details Axon's Service deliverables ("**SOW**"). In the event Axon provides an SOW to Agency, Axon is only responsible for the performance of Services described in the SOW. Additional services are out of scope. The Parties must document scope changes in a written and signed change order. Changes may require an equitable adjustment in fees or schedule. The SOW is incorporated into this Agreement by reference.

9. **Axon Device Warnings**. See www.axon.com/legal for the most current Axon Device warnings.

10. **Design Changes**. Axon may make design changes to any Axon Device or Service without notifying Agency or making the same change to Axon Devices and Services previously purchased by Agency.

11. **Bundled Offerings**. Some offerings in bundled offerings may not be generally available at the time of Agency's purchase. Axon will not provide a refund, credit, or additional discount beyond what is in the Quote due to a delay of availability or Agency's election not to utilize any portion of an Axon bundle.

12. **Insurance**. Axon will maintain General Liability, Workers' Compensation, and Automobile Liability insurance. Upon request, Axon will supply certificates of insurance.

13. **IP Rights**. Axon owns and reserves all right, title, and interest in Axon-manufactured Devices and Services and suggestions to Axon, including all related intellectual property rights. Agency will not cause any Axon proprietary rights to be violated.

14. **IP Indemnification**. Axon will indemnify Agency against all claims, losses, and reasonable expenses from any third-party claim alleging that the use of Axon-manufactured Devices or Services infringes or misappropriates the third-party's intellectual property rights. Agency must promptly provide Axon with written notice of such claim, tender to Axon the defense or settlement of such claim at Axon's expense and cooperate fully with Axon in the defense or settlement of such claim. Axon's IP indemnification obligations do not apply to claims based on (a) modification of Axon-manufactured Devices or Services by Agency or a third-party not approved by Axon; (b) use of Axon-manufactured Devices and Services in combination with hardware or services not approved by Axon; (c) use of Axon Devices and Services other than as permitted in this Agreement; or (d) use of Axon software that is not the most current release provided by Axon.

15. **Agency Responsibilities**. Agency is responsible for (a) Agency's use of Axon Devices; (b) breach of this Agreement or violation of applicable law by Agency or an Agency end user; (c) disputes between Agency and a third-party over Agency's use of Axon Devices; (d) ensuring Axon Devices are destroyed and disposed of securely and sustainably at Agency's cost; and (e) any regulatory violations or fines, as a result of improper destruction or disposal of Axon Devices.

16. **Termination**.

    16.1. **For Breach**. A Party may terminate this Agreement for cause if it provides thirty (30) days written notice of the breach to the other Party, and the breach remains uncured at the end of thirty (30) days. If Agency terminates this Agreement due to Axon's uncured breach, Axon will refund prepaid amounts on a prorated basis based on the effective date of termination.

    16.2. **By Agency**. If sufficient funds are not appropriated or otherwise legally available to pay the fees, Agency may terminate this Agreement. Agency will deliver notice of termination under this section as soon as reasonably practicable.

    16.3. **Effect of Termination**. Upon termination of this Agreement, Agency rights immediately terminate. Agency remains responsible for all fees incurred before the effective date of termination. If Agency purchases Axon Devices for less than the manufacturer's suggested retail price ("**MSRP**") and this Agreement terminates before the end of the Term, Axon will invoice Agency the difference between the MSRP for Axon Devices received, including any Spare Axon Devices, and amounts paid towards those Axon Devices. Only if terminating for non-appropriation, Agency may return Axon Devices to Axon within thirty (30) days of termination. MSRP is the standalone price of the individual Axon Device at the time of sale. For bundled Axon Devices, MSRP is the standalone price of all individual components.

17. **Confidentiality**. "**Confidential Information**" means nonpublic information designated as confidential or, given the nature of the information or circumstances surrounding disclosure, should reasonably be understood to be confidential. Each Party will take reasonable measures to avoid disclosure, dissemination, or unauthorized use of the other Party's Confidential Information. Unless required by law, neither Party will disclose the other Party's Confidential Information during the Term and for five (5) years thereafter. To the extent permissible by law, Axon pricing is Confidential Information and competition sensitive. If Agency receives a public records request to disclose Axon Confidential Information, to the extent allowed by law, Agency will provide notice to Axon before disclosure. Axon may publicly announce information related to this Agreement.

18. **General**.

18.1. **Force Majeure**. Neither Party will be liable for any delay or failure to perform due to a cause beyond a Party's reasonable control.

18.2. **Independent Contractors**. The Parties are independent contractors. Neither Party has the authority to bind the other. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties.

18.3. **Third-Party Beneficiaries**. There are no third-party beneficiaries under this Agreement.

18.4. **Non-Discrimination**. Neither Party nor its employees will discriminate against any person based on race; religion; creed; color; sex; gender identity and expression; pregnancy; childbirth; breastfeeding; medical conditions related to pregnancy, childbirth, or breastfeeding; sexual orientation; marital status; age; national origin; ancestry; genetic information; disability; veteran status; or any class protected by local, state, or federal law.

18.5. **Export Compliance**. Each Party will comply with all import and export control laws and regulations.

18.6. **Assignment**. Neither Party may assign this Agreement without the other Party's prior written consent. Axon may assign this Agreement, its rights, or obligations without consent: (a) to an affiliate or subsidiary; or (b) for purposes of financing, merger, acquisition, corporate reorganization, or sale of all or substantially all its assets. This Agreement is binding upon the Parties respective successors and assigns.

18.7. **Waiver**. No waiver or delay by either Party in exercising any right under this Agreement constitutes a waiver of that right.

18.8. **Severability**. If a court of competent jurisdiction holds any portion of this Agreement invalid or unenforceable, the remaining portions of this Agreement will remain in effect.

18.9. **Survival**. The following sections will survive termination: Payment, Warranty, Axon Device Warnings, Indemnification, IP Rights, and Agency Responsibilities.

18.10. **Governing Law**. The laws of the country, state, province, or municipality where Agency is physically located, without reference to conflict of law rules, govern this Agreement and any dispute arising from it. The United Nations Convention for the International Sale of Goods does not apply to this Agreement.

18.11. **Notices**. All notices must be in English. Notices posted on Agency's Axon Evidence site are effective upon posting. Notices by email are effective on the sent date of the email. Notices by personal delivery are effective immediately. Notices to Agency shall be provided to the address on file with Axon. Notices to Axon shall be provided to Axon Enterprise, Inc., Attn: Legal, 17800 North 85th Street, Scottsdale, Arizona 85255 with a copy to legal@axon.com.

18.12 **Entire Agreement**. This Agreement, including the Appendices and any SOW(s), represents the entire agreement between the Parties. This Agreement supersedes all prior agreements or understandings, whether written or verbal, regarding the subject matter of this Agreement. This Agreement may only be modified or amended in a writing signed by the Parties.

Each Party, by and through its respective representative authorized to execute this Agreement, has duly executed and delivered this Agreement as of the date of signature.

AXON:	**AGENCY**:
Axon Enterprise, Inc.	_____
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Axon Cloud Services Terms of Use Appendix

1. Definitions.

    a. **"Agency Content"** is data uploaded into, ingested by, or created in Axon Cloud Services within Agency's tenant, including media or multimedia uploaded into Axon Cloud Services by Agency. Agency Content includes Evidence but excludes Non-Content Data.

    b. "**Evidence**" is media or multimedia uploaded into Axon Evidence as 'evidence' by an Agency. Evidence is a subset of Agency Content.

    c. "**Non-Content Data**" is data, configuration, and usage information about Agency's Axon Cloud Services tenant, Axon Devices and client software, and users that is transmitted or generated when using Axon Devices. Non-Content Data includes data about users captured during account management and customer support activities. Non-Content Data does not include Agency Content.

    d. "**Personal Data**" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. **Access**. Upon Axon granting Agency a subscription to Axon Cloud Services, Agency may access and use Axon Cloud Services to store and manage Agency Content. Agency may not exceed more end users than the Quote specifies. Axon Air requires an Axon Evidence subscription for each drone operator. For Axon Evidence Lite, Agency may access and use Axon Evidence only to store and manage TASER CEW and TASER CAM data ("**TASER Data**"). Agency may not upload non-TASER Data to Axon Evidence Lite.

3. **Agency Owns Agency Content**. Agency controls and owns all right, title, and interest in Agency Content. Except as outlined herein, Axon obtains no interest in Agency Content, and Agency Content is not Axon's business records. Agency is solely responsible for uploading, sharing, managing, and deleting Agency Content. Axon will only have access to Agency Content for the limited purposes set forth herein. Agency agrees to allow Axon access to Agency Content to (a) perform troubleshooting, maintenance, or diagnostic screenings; and (b) enforce this Agreement or policies governing use of the Axon products.

4. **Security**. Axon will implement commercially reasonable and appropriate measures to secure Agency Content against accidental or unlawful loss, access or disclosure. Axon will maintain a comprehensive information security program to protect Axon Cloud Services and Agency Content including logical, physical access, vulnerability, risk, and configuration management; incident monitoring and response; encryption of uploaded digital evidence; security education; and data protection. Axon agrees to the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum.

5. **Agency Responsibilities**. Agency is responsible for (a) ensuring Agency owns Agency Content; (b) ensuring no Agency Content or Agency end user's use of Agency Content or Axon Cloud Services violates this Agreement or applicable laws; and (c) maintaining necessary computer equipment and Internet connections for use of Axon Cloud Services. If Agency becomes aware of any violation of this Agreement by an end user, Agency will immediately terminate that end user's access to Axon Cloud Services.

    a. Agency will also maintain the security of end usernames and passwords and security and access by end users to Agency Content. Agency is responsible for ensuring the configuration and utilization of Axon Cloud Services meet applicable Agency regulation and standards. Agency may not sell, transfer, or sublicense access to any other entity or person. Agency shall contact Axon immediately if an unauthorized party may be using Agency's account or Agency Content, or if account information is lost or stolen.

    b. To the extent Agency uses the Axon Cloud Services to interact with YouTube®, such use may be governed by the YouTube Terms of Service, available at https://www.youtube.com/static?template=terms.

6. **Privacy**. Agency's use of Axon Cloud Services is subject to the Axon Cloud Services Privacy Policy, a current version of which is available at https://www.axon.com/legal/cloud-services-privacy-policy. Agency agrees to allow Axon access to Non-Content Data from Agency to (a) perform troubleshooting, maintenance, or diagnostic

screenings; (b) provide, develop, improve, and support current and future Axon products and related services; and (c) enforce this Agreement or policies governing the use of Axon products.

7. **Axon Body 3 Wi-Fi Positioning**. Axon Body 3 cameras offer a feature to enhance location services where GPS/GNSS signals may not be available, for instance, within buildings or underground. Agency administrators can manage their choice to use this service within the administrative features of Axon Cloud Services. If Agency chooses to use this service, Axon must also enable the usage of the feature for Agency's Axon Cloud Services tenant. Agency will not see this option with Axon Cloud Services unless Axon has enabled Wi-Fi Positioning for Agency's Axon Cloud Services tenant. When Wi-Fi Positioning is enabled by both Axon and Agency, Non-Content and Personal Data will be sent to Skyhook Holdings, Inc. ("**Skyhook**") to facilitate the Wi-Fi Positioning functionality. Data controlled by Skyhook is outside the scope of the Axon Cloud Services Privacy Policy and is subject to the Skyhook Services Privacy Policy.

8. **Storage**. For Axon Unlimited Device Storage subscriptions, Agency may store unlimited data in Agency's Axon Evidence account only if data originates from Axon Capture or the applicable Axon Device. Axon may charge Agency additional fees for exceeding purchased storage amounts. Axon may place Agency Content that Agency has not viewed or accessed for six (6) months into archival storage. Agency Content in archival storage will not have immediate availability and may take up to twenty-four (24) hours to access.

   For Third-Party Unlimited Storage the following restrictions apply: (i) it may only be used in conjunction with a valid Axon's Evidence.com user license; (ii) is limited to data of the law enforcement agency that purchased the Third-Party Unlimited Storage and the Axon's Evidence.com end user or Agency is prohibited from storing data for other law enforcement agencies; and (iii) Agency may only upload and store data that is directly related to: (1) the investigation of, or the prosecution of a crime; (2) common law enforcement activities; or (3) any Agency Content created by Axon Devices or Evidence.com.

9. **Location of Storage**. Axon may transfer Agency Content to third-party subcontractors for storage. Axon will determine the locations of data centers for storage of Agency Content. For United States agencies, Axon will ensure all Agency Content stored in Axon Cloud Services remains within the United States. Ownership of Agency Content remains with Agency.

10. **Suspension**. Axon may temporarily suspend Agency's or any end user's right to access or use any portion or all of Axon Cloud Services immediately upon notice, if Agency or end user's use of or registration for Axon Cloud Services may (a) pose a security risk to Axon Cloud Services or any third-party; (b) adversely impact Axon Cloud Services, the systems, or content of any other customer; (c) subject Axon, Axon's affiliates, or any third-party to liability; or (d) be fraudulent. Agency remains responsible for all fees incurred through suspension. Axon will not delete Agency Content because of suspension, except as specified in this Agreement.

11. **Axon Cloud Services Warranty**. Axon disclaims any warranties or responsibility for data corruption or errors before Agency uploads data to Axon Cloud Services.

12. **Axon Records**. Axon Records is the software-as-a-service product that is generally available at the time Agency purchases an OSP 7 or OSP 10 bundle. During Agency's Axon Records Subscription Term, if any, Agency will be entitled to receive Axon's Update and Upgrade releases on an if-and-when available basis.

    a. The Axon Records Subscription Term will end upon the completion of the Axon Records Subscription as documented in the Quote, or if purchased as part of an OSP 7 or OSP 10 bundle, upon completion of the OSP 7 or OSP 10 Term ("**Axon Records Subscription**")

    b. An "**Update**" is a generally available release of Axon Records that Axon makes available from time to time. An "**Upgrade**" includes (i) new versions of Axon Records that enhance features and functionality, as solely determined by Axon; and/or (ii) new versions of Axon Records that provide additional features or perform additional functions. Upgrades exclude new products that Axon introduces and markets as distinct products or applications.

    c. New or additional Axon products and applications, as well as any Axon professional services needed to configure Axon Records, are not included. If Agency purchases Axon Records as part of a bundled offering, the Axon Record subscription begins on the later of the (1) start date of that bundled offering, or (2) date Axon provisions Axon Records to Agency.

    d. Users of Axon Records at the Agency may upload files to entities (incidents, reports, cases, etc) in Axon Records with no limit to the number of files and amount of storage. Notwithstanding the foregoing, Axon

may limit usage should the Agency exceed an average rate of one-hundred (100) GB per user per year of uploaded files. Axon will not bill for overages.

13. **Axon Cloud Services Restrictions**. Agency and Agency end users (including employees, contractors, agents, officers, volunteers, and directors), may not, or may not attempt to:

    a. copy, modify, tamper with, repair, or create derivative works of any part of Axon Cloud Services;

    b. reverse engineer, disassemble, or decompile Axon Cloud Services or apply any process to derive any source code included in Axon Cloud Services, or allow others to do the same;

    c. access or use Axon Cloud Services with the intent to gain unauthorized access, avoid incurring fees or exceeding usage limits or quotas;

    d. use trade secret information contained in Axon Cloud Services, except as expressly permitted in this Agreement;

    e. access Axon Cloud Services to build a competitive device or service or copy any features, functions, or graphics of Axon Cloud Services;

    f. remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon's or Axon's licensors on or within Axon Cloud Services; or

    g. use Axon Cloud Services to store or transmit infringing, libelous, or other unlawful or tortious material; material in violation of third-party privacy rights; or malicious code.

14. **After Termination**. Axon will not delete Agency Content for ninety (90) days following termination. There will be no functionality of Axon Cloud Services during these ninety (90) days other than the ability to retrieve Agency Content. Agency will not incur additional fees if Agency downloads Agency Content from Axon Cloud Services during this time. Axon has no obligation to maintain or provide Agency Content after these ninety (90) days and will thereafter, unless legally prohibited, delete all Agency Content. Upon request, Axon will provide written proof that Axon successfully deleted and fully removed all Agency Content from Axon Cloud Services.

15. **Post-Termination Assistance**. Axon will provide Agency with the same post-termination data retrieval assistance that Axon generally makes available to all customers. Requests for Axon to provide additional assistance in downloading or transferring Agency Content, including requests for Axon's data egress service, will result in additional fees and Axon will not warrant or guarantee data integrity or readability in the external system.

16. **U.S. Government Rights**. If Agency is a U.S. Federal department or using Axon Cloud Services on behalf of a U.S. Federal department, Axon Cloud Services is provided as a "commercial item," "commercial computer software," "commercial computer software documentation," and "technical data", as defined in the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement. If Agency is using Axon Cloud Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Agency will immediately discontinue use of Axon Cloud Services.

17. **Survival**. Upon any termination of this Agreement, the following sections in this Appendix will survive: Agency Owns Agency Content, Privacy, Storage, Axon Cloud Services Warranty, and Axon Cloud Services Restrictions.

Axon Customer Experience Improvement Program Appendix

1. **Axon Customer Experience Improvement Program (ACEIP)**. The ACEIP is designed to accelerate Axon's development of technology, such as building and supporting automated features, to ultimately increase safety within communities and drive efficiency in public safety. To this end, subject to the limitations on Axon as described below, Axon, where allowed by law, may make limited use of Agency Content from all of its customers to provide, develop, improve, and support current and future Axon products (collectively, "ACEIP Purposes"). However, at all times, Axon will comply with its obligations pursuant to the Axon Cloud Services Terms of Use Appendix to maintain a comprehensive data security program (including compliance with the CJIS Security Policy for Criminal Justice Information), privacy program, and data governance policy, including high industry standards of de-identifying Personal Data, to enforce its security and privacy obligations for the ACEIP. ACEIP has 2 tiers of participation, Tier 1 and Tier 2. By default, Agency will be a participant in ACEIP Tier 1. If Agency does not want to participate in ACEIP Tier 1, Agency can revoke its consent at any time. If Agency wants to participate in Tier 2, as detailed below, Agency can check the ACEIP Tier 2 box below. If Agency does not want to participate in ACEIP Tier 2, Agency should leave box unchecked. At any time, Agency may revoke its consent to ACEIP Tier 1, Tier 2, or both Tiers.

2. **ACEIP Tier 1.**

   2.1. When Axon uses Agency Content for the ACEIP Purposes, Axon will extract from Agency Content and may store separately copies of certain segments or elements of the Agency Content (collectively, "**ACEIP Content**"). When extracting ACEIP Content, Axon will use commercially reasonable efforts to aggregate, transform or de-identify Agency Content so that the extracted ACEIP Content is no longer reasonably capable of being associated with, or could reasonably be linked directly or indirectly to a particular individual ("**Privacy Preserving Technique(s)**"). For illustrative purposes, some examples are described in footnote 1[1]. For clarity, ACEIP Content will still be linked indirectly, with an attribution, to the Agency from which it was extracted. This attribution will be stored separately from the data itself, but is necessary for and will be solely used to enable Axon to identify and delete all ACEIP Content upon Agency request. Once de-identified, ACEIP Content may then be further modified, analyzed, and used to create derivative works. At any time, Agency may revoke the consent granted herein to Axon to access and use Agency Content for ACEIP Purposes. Within 30 days of receiving the Agency's request, Axon will no longer access or use Agency Content for ACEIP Purposes and will delete any and all ACEIP Content. Axon will also delete any derivative works which may reasonably be capable of being associated with, or could reasonably be linked directly or indirectly to Agency. In addition, if Axon uses Agency Content for the ACEIP Purposes, upon request, Axon will make available to Agency a list of the specific type of Agency Content being used to generate ACEIP Content, the purpose of such use, and the retention, privacy preserving extraction technique, and relevant data protection practices applicable to the Agency Content or ACEIP Content ("**Use Case**"). From time to time, Axon may develop and deploy new Use Cases. At least 30 days prior to authorizing the deployment of any new Use Case, Axon will provide Agency notice (by updating the list of Use Case at https://www.axon.com/aceip and providing Agency with a mechanism to obtain notice of that update or another commercially reasonable method to Agency designated contact) ("**New Use Case**").

   2.2. **Expiration of ACEIP Tier 1**. Agency consent granted herein will expire upon termination of the Agreement. In accordance with section 1.1.1, within 30 days of receiving the Agency's request, Axon will no longer access or use Agency Content for ACEIP Purposes and will delete ACEIP Content. Axon will also delete any derivative works which may reasonably be capable of being associated with, or could reasonably be linked directly or indirectly to, Agency.

3. **ACEIP Tier 2**. In addition to ACEIP Tier 1, if Agency wants to help further improve Axon's services, Agency may choose to participate in Tier 2 of the ACEIP. ACEIP Tier 2 grants Axon certain additional rights to use Agency Content, in addition to those set forth in Tier 1 above, without the guaranteed deployment of a Privacy Preserving Technique

[1] For example; (a) when extracting specific text to improve automated transcription capabilities, text that could be used to directly identify a particular individual would not be extracted, and extracted text would be disassociated from identifying metadata of any speakers, and the extracted text would be split into individual words and aggregated with other data sources (including publicly available data) to remove any reasonable ability to link any specific text directly or indirectly back to a particular individual; (b) when extracting license plate data to improve Automated License Plate Recognition (ALPR) capabilities, individual license plate characters would be extracted and disassociated from each other so a complete plate could not be reconstituted, and all association to other elements of the source video, such as the vehicle, location, time, and the surrounding environment would also be removed; (c) when extracting audio of potential acoustic events (such as glass breaking or gun shots), very short segments (<1 second) of audio that only contains the likely acoustic events would be extracted and all human utterances would be removed.

to enable product development, improvement, and support that cannot be accomplished with aggregated, transformed, or de-identified data.

☐ Check this box if Agency wants to help further improve Axon's services by participating in ACEIP Tier 2 in addition to Tier 1. Axon will not enroll Agency into ACEIP Tier 2 until Axon and Agency agree to terms in writing providing for such participation in ACEIP Tier 2.

Technology Assurance Plan Appendix

If Technology Assurance Plan ("**TAP**") or a bundle including TAP is on the Quote, this appendix applies.

1. **TAP Warranty**. The TAP warranty is an extended warranty that starts at the end of the one- (1-) year hardware limited warranty.

2. **Officer Safety Plan**. If Agency purchases an Officer Safety Plan ("**OSP**"), Agency will receive the deliverables detailed in the Quote. Agency must accept delivery of the TASER CEW and accessories as soon as available from Axon.

3. **OSP 7 or OSP 10 Term**. OSP 7 or OSP 10 begins on the date specified in the Quote ("**OSP Term**").

4. **TAP BWC Upgrade**. If Agency has no outstanding payment obligations and purchased TAP, Axon will provide Agency a new Axon body-worn camera ("**BWC Upgrade**") as scheduled in the Quote. If Agency purchased TAP, Axon will provide a BWC Upgrade that is the same or like Axon Device, at Axon's option. Axon makes no guarantee the BWC Upgrade will utilize the same accessories or Axon Dock.

5. **TAP Dock Upgrade**. If Agency has no outstanding payment obligations and purchased TAP, Axon will provide Agency a new Axon Dock as scheduled in the Quote ("**Dock Upgrade**"). Accessories associated with any Dock Upgrades are subject to change at Axon discretion. Dock Upgrades will only include a new Axon Dock bay configuration unless a new Axon Dock core is required for BWC compatibility. If Agency originally purchased a single-bay Axon Dock, the Dock Upgrade will be a single-bay Axon Dock model that is the same or like Axon Device, at Axon's option. If Agency originally purchased a multi-bay Axon Dock, the Dock Upgrade will be a multi-bay Axon Dock that is the same or like Axon Device, at Axon's option.

6. **Upgrade Delay**. Axon may ship the BWC and Dock Upgrades as scheduled in the Quote without prior confirmation from Agency unless the Parties agree in writing otherwise at least ninety (90) days in advance. Axon may ship the final BWC and Dock Upgrade as scheduled in the Quote sixty (60) days before the end of the Subscription Term without prior confirmation from Agency.

7. **Upgrade Change**. If Agency wants to upgrade Axon Device models from the current Axon Device to an upgraded Axon Device, Agency must pay the price difference between the MSRP for the current Axon Device and the MSRP for the upgraded Axon Device. If the model Agency desires has an MSRP less than the MSRP of the offered BWC Upgrade or Dock Upgrade, Axon will not provide a refund. The MSRP is the MSRP in effect at the time of the upgrade.

8. **Return of Original Axon Device**. Within thirty (30) days of receiving a BWC or Dock Upgrade, Agency must return the original Axon Devices to Axon or destroy the Axon Devices and provide a certificate of destruction to Axon including serial numbers for the destroyed Axon Devices. If Agency does not return or destroy the Axon Devices, Axon will deactivate the serial numbers for the Axon Devices received by Agency.

9. **Termination**. If Agency's payment for TAP, OSP, or Axon Evidence is more than thirty (30) days past due, Axon may terminate TAP or OSP. Once TAP or OSP terminates for any reason:

   9.1. TAP and OSP coverage terminate as of the date of termination and no refunds will be given.

   9.2. Axon will not and has no obligation to provide the Upgrade Models.

   9.3. Agency must make any missed payments due to the termination before Agency may purchase any future TAP or OSP.

Axon Auto-Tagging Appendix

If Auto-Tagging is included on the Quote, this Appendix applies.

1. **Scope.** Axon Auto-Tagging consists of the development of a module to allow Axon Evidence to interact with Agency's Computer-Aided Dispatch ("**CAD**") or Records Management Systems ("**RMS**"). This allows end users to auto-populate Axon video meta-data with a case ID, category, and location-based on data maintained in Agency's CAD or RMS.

2. **Support**. For thirty (30) days after completing Auto-Tagging Services, Axon will provide up to five (5) hours of remote support at no additional charge. Axon will provide free support due to a change in Axon Evidence, if Agency maintains an Axon Evidence and Auto-Tagging subscription. Axon will not provide support if a change is required because Agency changes its CAD or RMS.

3. **Changes**. Axon is only responsible to perform the Services in this Appendix. Any additional Services are out of scope. The Parties must document scope changes in a written and signed change order. Changes may require an equitable adjustment in fees or schedule.

4. **Agency Responsibilities**. Axon's performance of Auto-Tagging Services requires Agency to:

   4.1. Make available relevant systems, including Agency's current CAD or RMS, for assessment by Axon (including remote access if possible);

   4.2. Make required modifications, upgrades or alterations to Agency's hardware, facilities, systems and networks related to Axon's performance of Auto-Tagging Services;

   4.3. Provide access to the premises where Axon is performing Auto-Tagging Services, subject to Agency safety and security restrictions, and allow Axon to enter and exit the premises with laptops and materials needed to perform Auto-Tagging Services;

   4.4. Provide all infrastructure and software information (TCP/IP addresses, node names, network configuration) necessary for Axon to provide Auto-Tagging Services;

   4.5. Promptly install and implement any software updates provided by Axon;

   4.6. Ensure that all appropriate data backups are performed;

   4.7. Provide assistance, participation, and approvals in testing Auto-Tagging Services;

   4.8. Provide Axon with remote access to Agency's Axon Evidence account when required;

   4.9. Notify Axon of any network or machine maintenance that may impact the performance of the module at Agency; and

   4.10. Ensure reasonable availability of knowledgeable staff and personnel to provide timely, accurate, complete, and up-to-date documentation and information to Axon.

5. **Access to Systems**. Agency authorizes Axon to access Agency's relevant computers, network systems, and CAD or RMS solely for performing Auto-Tagging Services. Axon will work diligently to identify the resources and information Axon expects to use and will provide an initial list to Agency. Agency is responsible for and assumes the risk of any problems, delays, losses, claims, or expenses resulting from the content, accuracy, completeness, and consistency of all data, materials, and information supplied by Agency.

Axon Respond Appendix

This Axon Respond Appendix applies to both Axon Respond and Axon Respond Plus, if either is included on the Quote.

1. **Axon Respond Subscription Term**. If Agency purchases Axon Respond as part of a bundled offering, the Axon Respond subscription begins on the later of the (1) start date of that bundled offering, or (2) date Axon provisions Axon Respond to Agency. If Agency purchases Axon Respond as a standalone, the Axon Respond subscription begins the later of the (1) date Axon provisions Axon Respond to Agency, or (2) first day of the month following the Effective Date. The Axon Respond subscription term will end upon the completion of the Axon Evidence Subscription associated with Axon Respond.

2. **Scope of Axon Respond**. The scope of Axon Respond is to assist Agency with real-time situational awareness during critical incidents to improve officer safety, effectiveness, and awareness. In the event Agency uses Axon Respond outside this scope, Axon may initiate good-faith discussions with Agency on upgrading Agency's Axon Respond to better meet Agency's needs.

3. **Axon Body 3 LTE Requirements**. Axon Respond is only available and usable with an LTE enabled body-worn camera. Axon is not liable if Agency utilizes the LTE device outside of the coverage area or if the LTE carrier is unavailable. LTE coverage is only available in the United States, including any U.S. territories. Axon may utilize a carrier of Axon's choice to provide LTE service. Axon may change LTE carriers during the Term without Agency's consent.

4. **Axon Fleet 3 LTE Requirements.** Axon Respond is only available and usable with a Fleet 3 system configured with LTE modem and service. Agency is responsible for providing LTE service for the modem. Coverage and availability of LTE service is subject to Agency's LTE carrier.

5. **Axon Respond Service Limitations**. Agency acknowledges that LTE service is made available only within the operating range of the networks. Service may be temporarily refused, interrupted, or limited because of: (a) facilities limitations; (b) transmission limitations caused by atmospheric, terrain, other natural or artificial conditions adversely affecting transmission, weak batteries, system overcapacity, movement outside a service area or gaps in coverage in a service area, and other causes reasonably outside of the carrier's control such as intentional or negligent acts of third parties that damage or impair the network or disrupt service; or (c) equipment modifications, upgrades, relocations, repairs, and other similar activities necessary for the proper or improved operation of service.

    5.1. With regard to Axon Body 3, Partner networks are made available as-is and the carrier makes no warranties or representations as to the availability or quality of roaming service provided by carrier partners, and the carrier will not be liable in any capacity for any errors, outages, or failures of carrier partner networks. Agency expressly understands and agrees that it has no contractual relationship whatsoever with the underlying wireless service provider or its affiliates or contractors and Agency is not a third-party beneficiary of any agreement between Axon and the underlying carrier.

6. **Termination**. Upon termination of this Agreement, or if Agency stops paying for Axon Respond or bundles that include Axon Respond, Axon will end Axon Respond services, including any Axon-provided LTE service.

Add-on Services Appendix

This Appendix applies if Axon Community Request, Axon Redaction Assistant, and/or Axon Performance are included on the Quote.

1. **Subscription Term**. If Agency purchases Axon Community Request, Axon Redaction Assistant, or Axon Performance as part of OSP 7 or OSP 10, the subscription begins on the later of the (1) start date of the OSP 7 or OSP 10 Term, or (2) date Axon provisions Axon Community Request Axon Redaction Assistant, or Axon Performance to Agency.

1.1. If Agency purchases Axon Community Request, Axon Redaction Assistant, or Axon Performance as a standalone, the subscription begins the later of the (1) date Axon provisions Axon Community Request, Axon Redaction Assistant, or Axon Performance to Agency, or (2) first day of the month following the Effective Date.

1.2. The subscription term will end upon the completion of the Axon Evidence Subscription associated with the add-on.

2. **Axon Community Request Storage**. For Axon Community Request, Agency may store an unlimited amount of data submitted through the public portal ("**Portal Content**"), within Agency's Axon Evidence instance. The post-termination provisions outlined in the Axon Cloud Services Terms of Use Appendix also apply to Portal Content.

3. **Performance Auto-Tagging Data**. In order to provide some features of Axon Performance to Agency, Axon will need to store call for service data from Agency's CAD or RMS.

Axon Application Programming Interface Appendix

This Appendix applies if Axon's API Services are included on the Quote.

1. **Definitions**.

   1.1. "**API Client**" means the software that acts as the interface between Agency's computer and the server, which is already developed or to be developed by Agency.

   1.2. "**API Interface**" means software implemented by Agency to configure Agency's independent API Client Software to operate in conjunction with the API Service for Agency's authorized Use.

   1.3. "**Axon Evidence Partner API, API or Axon API**" (collectively "**API Service**") means Axon's API which provides a programmatic means to access data in Agency's Axon Evidence account or integrate Agency's Axon Evidence account with other systems.

   1.4. "**Use**" means any operation on Agency's data enabled by the supported API functionality.

2. **Purpose and License**.

   2.1. Agency may use API Service and data made available through API Service, in connection with an API Client developed by Agency. Axon may monitor Agency's use of API Service to ensure quality, improve Axon devices and services, and verify compliance with this Agreement. Agency agrees to not interfere with such monitoring or obscure from Axon Agency's use of API Service. Agency will not use API Service for commercial use.

   2.2. Axon grants Agency a non-exclusive, non-transferable, non-sublicensable, worldwide, revocable right and license during the Term to use API Service, solely for Agency's Use in connection with Agency's API Client.

   2.3. Axon reserves the right to set limitations on Agency's use of the API Service, such as a quota on operations, to ensure stability and availability of Axon's API. Axon will use reasonable efforts to accommodate use beyond the designated limits.

3. **Configuration**. Agency will work independently to configure Agency's API Client with API Service for Agency's applicable Use. Agency will be required to provide certain information (such as identification or contact details) as part of the registration. Registration information provided to Axon must be accurate. Agency will inform Axon promptly of any updates. Upon Agency's registration, Axon will provide documentation outlining API Service information.

4. **Agency Responsibilities**. When using API Service, Agency and its end users may not:

   4.1. use API Service in any way other than as expressly permitted under this Agreement;

   4.2. use in any way that results in, or could result in, any security breach to Axon;

   4.3. perform an action with the intent of introducing any viruses, worms, defect, Trojan horses, malware, or any items of a destructive nature to Axon Devices and Services;

   4.4. interfere with, modify, disrupt or disable features or functionality of API Service or the servers or networks providing API Service;

   4.5. reverse engineer, decompile, disassemble, or translate or attempt to extract the source code from API Service or any related software;

   4.6. create an API Interface that functions substantially the same as API Service and offer it for use by third parties;

   4.7. provide use of API Service on a service bureau, rental or managed services basis or permit other individuals or entities to create links to API Service;

   4.8. frame or mirror API Service on any other server, or wireless or Internet-based device;

   4.9. make available to a third-party, any token, key, password or other login credentials to API Service;

   4.10. take any action or inaction resulting in illegal, unauthorized or improper purposes; or

   4.11. disclose Axon's API manual.

5. **API Content**. All content related to API Service, other than Agency Content or Agency's API Client content, is considered Axon's API Content, including:

   5.1. the design, structure and naming of API Service fields in all responses and requests;

5.2. the resources available within API Service for which Agency takes actions on, such as evidence, cases, users, or reports;

5.3. the structure of and relationship of API Service resources; and

5.4. the design of API Service, in any part or as a whole.

6. **Prohibitions on API Content**. Neither Agency nor its end users will use API content returned from the API Interface to:

6.1. scrape, build databases, or otherwise create permanent copies of such content, or keep cached copies longer than permitted by the cache header;

6.2. copy, translate, modify, create a derivative work of, sell, lease, lend, convey, distribute, publicly display, or sublicense to any third-party;

6.3. misrepresent the source or ownership; or

6.4. remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices).

7. **API Updates**. Axon may update or modify the API Service from time to time ("**API Update**"). Agency is required to implement and use the most current version of API Service and to make any applicable changes to Agency's API Client required as a result of such API Update. API Updates may adversely affect how Agency's API Client access or communicate with API Service or the API Interface. Each API Client must contain means for Agency to update API Client to the most current version of API Service. Axon will provide support for one (1) year following the release of an API Update for all depreciated API Service versions.

ATTACHMENT 1

Pricing Schedule

SECTION A: HARDWARE

Item No.	Description	Proposer Description	Cost per Unit
1	Camera in specified configuration	Model #: Axon Body 3 Camera Axon will deliver 2,118 cameras at $0 as TAP (Technology Assurance Plan) replacement for existing contract. (An additional 63 spare cameras will be provided) Each Axon Body 3 Camera includes one body camera mount (The city has previously used Magnet and Molle Mounts), and a USB-C charging cable. If the City wishes to procure additional Axon Body 3 Cameras beyond the eligible TAP quantity of 2,118, the cost per camera is $749	$0 - $749
2	Optional Camera Type	Model #: Axon Flex 2 POV Camera The Axon Flex 2 is a small point of view camera often utilized in specialized units (e.g., SWAT) as a non-chest mounted camera option. The cost per camera is $732. Each Flex 2 Camera includes one camera mount. Model #: Axon Body 4 Camera The Axon Body 4 Camera was recently released in July 2023. As part of the TAP program listed in the previous response, the Agency is given the option to select the camera to accept for TAP. San Diego Police Department is eligible to take 2,118	$732 - $849*

Item No.	Description	Proposer Description	Cost per Unit
		cameras at $0 for the TAP replacement. (An additional 63 spare cameras will be provided) Each Axon Body 4 Camera includes one mount as described above. If the City wishes to procure additional Axon Body 4 Cameras beyond the eligible TAP quantity of 2,118, the cost per camera is $849	
3	BWC Dock (Multi Camera)	Axon will deliver (248) 8-Bay Docks at $0 as TAP replacement for existing contract. The Axon 8-Bay Dock Bundle includes the 8-Bay Dock and charging accessories. If the City wishes to procure additional 8-Bay Docks beyond the referenced quantities, the cost per dock is $1,595. This is the cost for Axon Body 3 or Axon Body 4 docks.	$1,595*
4	BWC Dock (Single Camera)	Axon will deliver (16) 1-Bay Docks at $0 as TAP replacement for existing contract. The Axon 1-Bay Dock Bundle includes the 1-Bay Dock and charging accessories. If the City wishes to procure additional 1-Bay Docks beyond the referenced quantities, the cost per dock is $229	$229*

Item No.	Description	Proposer Description	Cost per Unit
5	BWC Dock (Optional Camera)	The Axon Flex 2 6-Bay Charging Dock Bundle includes the 6-Bay Dock and charging accessories.	$1606.90*
6	BWC Mount (Std. Patrol)	Each Axon Body 3 Camera includes one body camera mount (The city has previously used Magnet and Molle Mounts), and a USB-C charging cable at no additional cost. If the City wishes to purchase additional mounts the cost is $31.30	$31.30*
7	BWC Mount (MOLLE)	Each Axon Body 3 Camera includes two body camera mounts (The city has previously used Magnet and Molle Mounts), and a USB-C charging cable at no additional cost. If the City wishes to purchase additional mounts the cost is $31.30	$31.30*
8	BWC Mount (Other)	Each Axon Body 3 Camera includes one body camera mount (The city has previously used Magnet and Molle Mounts), and a USB-C charging cable at no additional cost If the City wishes to purchase additional mounts the cost range is $18 to $43, depending on the mount selected.	$18 - $43
			$0*

Total Cost for Section A:

*For the 2,118 cameras that are currently provided with the TAP refresh.

$138,385 for additional Body 3 or Body 4 cameras for the additional 132 cameras and corresponding docks to bring the total camera count to 2,250

SECTION B: STORAGE/ VIDEO MANAGEMENT (VM)

Item No.	Description	Proposer Description (What is included, i.e., maintenance and support, training)	Cost per Camera
1	VM Software Licensing	Axon Body 3 Unlimited + TAP Program: Included in the AB3 Unlimited + TAP Bundle is a Professional Axon Evidence (Evidence.com) user license, Unlimited Axon Device Storage, 10 GB ala carte third party storage, extended warranty on the BWC and Dock for the five-year term, two (2) BWC hardware refresh/replacements, and two (2) Dock hardware refresh/replacements	$89 Per User, Per Month
2	Integration Licensing	Axon doesn't anticipate the City needing an integration license. If the City chooses to implement an integration, the service is $35,000 with an annual support and maintenance at $5,000. Axon doesn't anticipate the City needing Data Conversion or Migration Services. If the City chooses to implement a migration service, the migration is $35,000 per migration channel. *This is separate from Axon Auto-Tagging as requested below.	$0
3	Unlimited Storage	Included in the AB3 Unlimited + TAP Bundle is Unlimited Axon Device (1st Party) Storage. *If the City wishes to consider a full Unlimited 3rd Party Storage Plan, allowing the City to have a true unlimited storage plan for third party data (e.g. drone video, crime scene photos, cell phone extractions, etc.) the cost is $29.00 per user, per month.	$0

Item No.	Description	Proposer Description (What is included, i.e., maintenance and support, training)	Cost per Camera
4	*Package Solution #1	Axon has typically provided a Basic License Bundle to the City for additional users who might not wear a body camera, but require access to Axon Evidence (Evidence.com). The Basic License Bundle includes 10 GB ala carte storage, and the basic user license.	$17 Per User, Per Month
5	*Package Solution #2	Axon has typically provided a Professional License Bundle to the City for additional users who might not wear a body camera, but require additional access to Axon Evidence (Evidence.com). The Professional License Bundle includes 10 GB ala carte storage and the professional license granting access to Pro Features in Axon Evidence.	$42 Per User, Per Month
6	*Package Solution #3	For the City's consideration, Axon can provide a packaged solution that includes both the Taser (CEW) and Body Worn Camera in one unified license. The Officer Safety Program (OSP10+) includes the following: Taser 7 or 10 Certification Bundle, Signal Sidearm, Respond for Devices, Unlimited Evidence Licensing (BWC), Auto-Tagging, Redaction Assistant, 100 GB Third Party Data Storage per User, Migration Services, Third Party Video Support, Performance, Citizen for Communities, and Professional Standards. This package also includes 5 year extended warranty, and two refresh/replacements on all body worn camera and dock hardware.	$229 or 239 Per User, Per Month (OSP7+ or 10+)

Item No.	Description	Proposer Description (What is included, i.e., maintenance and support, training)	Cost per Camera
7	*Package Solution #4	An alternate offering to "Package Solution #3" is Officer Safety Plan 7 or 10 which includes Taser 7 or 10 Certification Bundle, Unlimited Evidence Licensing (BWC), Signal Sidearm, Respond (map), and Standards. The cost per user, per month ranges from $166 - $176 based upon Taser platform.	$166 or $176 Per User, Per Month (OSP 7 or 10)
			$89 Per User, Per Month* (BWC Unlimited)

Total Cost for Section B:

*Optional additional basic and/or pro licenses as desired. Full Axon Package Solutions range from $166 to $239 Per User, Per Month

Section A - Hardware Total Cost:	$ 0.00 for 2,118 body worn cameras. Additional camera costs listed above.
Section B - Storage/Video Management Total Cost:	$ 89.00 Per User, Per Month for BWC Unlimited* (Optional plans listed above)
Sections A & B Total Cost:	$ 89.00 Per User, Per Month for BWC Unlimited and camera costs for quantities beyond 2,118 cameras.

***Clearly describe what is included in these services. This may include pricing program discounts/package solutions offering a variety of selected equipment, licensing fees, extended warranty plans, or other available services that would maximize cost effectiveness.**

List any additional required hardware or software items not covered above in the table below to meet the City's specifications described in this RFP. The City will consider it as part of this procurement.

Item No.	Description	Proposer Description	Cost per Unit
1			$

Optional Features – Proposers must have the following additional add-on features available for purchase by the City.

Item No.	Description	Proposer Description	Cost per Camera
1	Automatic Video Tagging	Automatic Video Tagging, or Auto-Tagging is currently deployed by the City and automatically tags body worn camera video with the appropriate Call for Service metadata from the City's CAD or RMS System.	$9 Per User, Per Month *Required across sworn count
2	Audio/Video Redaction	Audio and Video Redaction is included in our Redaction Studio included with a Pro License. Redaction Assistant speeds up the redaction process by automating redactions for common objects like faces, license plates, and video screens (e.g., MDT screens). The cost notated here is for Redaction Assistant Studio.	$9 Per User, Per Month *Required across sworn count
3	Live Feed	Axon Respond builds on the active intelligence provided by the AB3 LTE connected camera and will support live video streaming from the AB3 camera, critical evidence previews, and prioritized wireless upload. Map based location tracking is also available to support improved situational awareness	$19 Per User, Per Month *Required across sworn count
4	"Automatic On" Activation Feature	Axon assumes the City is referring to "Remote Activation" as "Automatic On". If so, remote activation is included with the purchase or Respond+ or "Live Feed" as described above. There is an integration set-up cost of $5,000 for professional services. Additional "automatic on" solutions can be accomplished via signal technology. This includes a configuration setting on our latest taser models, signal device for vehicle, or signal sidearm.	$5,000 for setup Signal sidearm or signal vehicle are available for $249 per device

	Performance	Performance allows the agency to monitor the health and status of the body camera program. Data is provided via dashboards so administrators can quickly understand the utilization metrics of the program based upon division/team, etc. In addition, supervisors can require random video reviews and track the compliance with conducting reviews.	$10 Per User, Per Month *Required across sworn count

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-462591-45251.787MH

Issued: 11/21/2023

Quote Expiration: 12/31/2023

Estimated Contract Start Date: 01/01/2024

Account Number: 105252

Payment Terms: N30

Delivery Method:

SHIP TO	BILL TO
Business;Delivery;Invoice-1401 Broadway 1401 Broadway San Diego, CA 92101-5710 USA	San Diego Police Dept. - CA 1401 BROADWAY SAN DIEGO CA 92101-5710 USA Email:

SALES REPRESENTATIVE	PRIMARY CONTACT
Megan Hardisty Phone: +1 4802537854 Email: mhardisty@axon.com Fax:	Lisa McKean Phone: (619) 531-2113 Email: lmckean@pd.sandiego.gov Fax:

Quote Summary

Program Length	60 Months
TOTAL COST	$11,804,310.40
ESTIMATED TOTAL W/ TAX	$12,099,384.45

Discount Summary

Average Savings Per Year	$1,035,856.18
TOTAL SAVINGS	$5,179,280.90

Payment Summary

Date	Subtotal	Tax	Total
Jan 2024	$1,161,814.70	$29,042.04	$1,190,856.74
Jul 2024	$2,105,000.00	$52,618.99	$2,157,618.99
Jul 2025	$2,275,000.00	$56,868.48	$2,331,868.48
Jul 2026	$2,350,000.00	$58,743.28	$2,408,743.28
Jul 2027	$2,385,000.00	$59,618.19	$2,444,618.19

Payment Summary

Date	Subtotal	Tax	Total
Jul 2028	$1,527,495.70	$38,183.07	$1,565,678.77
Total	**$11,804,310.40**	**$295,074.05**	**$12,099,384.45**

Quote Unbundled Price:	**$16,983,591.30**
Quote List Price:	**$15,151,078.50**
Quote Subtotal:	**$11,804,310.40**

Pricing

All deliverables are detailed in Delivery Schedules section lower in proposal

Item	Description	Qty	Term	Unbundled	List Price	Net Price	Subtotal	Tax	Total
Program									
BWCUwTAP	BWC Unlimited with TAP	1954	60	$114.19	$98.58	$89.00	$10,434,360.00	$293,578.56	$10,727,938.56
T00001	AB4 FLEX POV TAP BUNDLE	15	60	$6.74	$7.04	$6.74	$6,066.00	$364.31	$6,430.31
BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	60	$13.94	$11.92	$11.92	$15,734.40	$740.73	$16,475.13
A la Carte Hardware									
74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150			$31.30	$0.00	$0.00	$0.00	$0.00
H00001	AB4 Camera Bundle	1954	60		$849.00	$0.00	$0.00	$0.00	$0.00
H00002	AB4 Multi Bay Dock Bundle	245	60		$1,638.90	$0.00	$0.00	$0.00	$0.00
H00004	AB4 FLEX POV HARDWARE BUNDLE	15	60		$249.00	$0.00	$0.00	$0.00	$0.00
H00003	AB4 1-Bay Dock Bundle	22	60		$229.00	$3.82	$5,038.00	$390.45	$5,428.45
A la Carte Software									
73682	AUTO TAGGING LICENSE	1954	60		$9.76	$9.00	$1,055,160.00	$0.00	$1,055,160.00
ProLicense	Pro License Bundle	50	60		$42.91	$42.00	$126,000.00	$0.00	$126,000.00
BasicLicense	Basic License Bundle	160	60		$16.87	$16.87	$161,952.00	$0.00	$161,952.00
Total							**$11,804,310.40**	**$295,074.05**	**$12,099,384.45**

Delivery Schedule

Hardware

Bundle	Item	Description	QTY	Estimated Delivery Date
AB4 1-Bay Dock Bundle	100201	AXON BODY 4 - 1 BAY DOCK	22	12/01/2023
AB4 1-Bay Dock Bundle	71104	NORTH AMER POWER CORD FOR AB3 & T7 1-BAY DOCK/DATAPORT	22	12/01/2023
AB4 Camera Bundle	100147	AXON BODY 4 - NA - US FIRST RESPONDER - BLK - RAPIDLOCK	1954	12/01/2023
AB4 Camera Bundle	100147	AXON BODY 4 - NA - US FIRST RESPONDER - BLK - RAPIDLOCK	65	12/01/2023
AB4 Camera Bundle	100466	USB-C to USB-C CABLE FOR AB4	2150	12/01/2023
AB4 Camera Bundle	11507	MOLLE MOUNT, SINGLE, AXON RAPIDLOCK	2150	12/01/2023
AB4 FLEX POV HARDWARE BUNDLE	100200	AB4 FLEX POV MODULE	15	12/01/2023
AB4 FLEX POV HARDWARE BUNDLE	100852	AXON BODY 4 POV C-CLIP	15	12/01/2023
AB4 FLEX POV HARDWARE BUNDLE	100858	AXON BODY 4 POV UNIVERSAL HELMET MOUNT	17	12/01/2023
AB4 FLEX POV HARDWARE BUNDLE	100958	AB4 FLEX POV MODULE CABLE 48 IN.	15	12/01/2023
AB4 Multi Bay Dock Bundle	100206	AXON BODY 4 - 8 BAY DOCK	245	12/01/2023
AB4 Multi Bay Dock Bundle	70033	WALL MOUNT BRACKET, ASSY, EVIDENCE.COM DOCK	245	12/01/2023
AB4 Multi Bay Dock Bundle	71019	NORTH AMER POWER CORD FOR AB3 8-BAY, AB2 1-BAY / 6-BAY DOCK	245	12/01/2023
A la Carte	74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150	12/01/2023
Body Worn Camera Single-Bay Dock TAP Bundle	73313	1-BAY DOCK AXON CAMERA REFRESH ONE	22	06/01/2026
BWC Unlimited with TAP	73309	AXON CAMERA REFRESH ONE	2019	06/01/2026
BWC Unlimited with TAP	73689	MULTI-BAY BWC DOCK 1ST REFRESH	245	06/01/2026
AB4 FLEX POV TAP BUNDLE	100976	AB4 FLEX POV REFRESH ONE	15	12/01/2028
Body Worn Camera Single-Bay Dock TAP Bundle	73314	1-BAY DOCK AXON CAMERA REFRESH TWO	22	12/01/2028
BWC Unlimited with TAP	73310	AXON CAMERA REFRESH TWO	2019	12/01/2028
BWC Unlimited with TAP	73688	MULTI-BAY BWC DOCK 2ND REFRESH	245	12/01/2028

Software

Bundle	Item	Description	QTY	Estimated Start Date	Estimated End Date
Basic License Bundle	73683	10 GB EVIDENCE.COM A-LA-CART STORAGE	160	01/01/2024	12/31/2028
Basic License Bundle	73840	EVIDENCE.COM BASIC ACCESS LICENSE	160	01/01/2024	12/31/2028
BWC Unlimited with TAP	73686	EVIDENCE.COM UNLIMITED AXON DEVICE STORAGE	1954	01/01/2024	12/31/2028
BWC Unlimited with TAP	73746	PROFESSIONAL EVIDENCE.COM LICENSE	1954	01/01/2024	12/31/2028
Pro License Bundle	73683	10 GB EVIDENCE.COM A-LA-CART STORAGE	150	01/01/2024	12/31/2028
Pro License Bundle	73746	PROFESSIONAL EVIDENCE.COM LICENSE	50	01/01/2024	12/31/2028
A la Carte	73682	AUTO TAGGING LICENSE	1954	01/01/2024	12/31/2028

Warranties

Bundle	Item	Description	QTY	Estimated Start Date	Estimated End Date
BWC Unlimited with TAP	80464	EXT WARRANTY, CAMERA (TAP)	1954	01/01/2024	12/31/2028
BWC Unlimited with TAP	80464	EXT WARRANTY, CAMERA (TAP)	65	01/01/2024	12/31/2028
AB4 FLEX POV TAP BUNDLE	100945	EXT WARRANTY, AB4 FLEX POV MODULE	15	12/01/2024	12/31/2028
Body Worn Camera Single-Bay Dock TAP Bundle	80466	EXT WARRANTY, SINGLE-BAY DOCK (TAP)	22	12/01/2024	12/31/2028
BWC Unlimited with TAP	80465	EXT WARRANTY, MULTI-BAY DOCK (TAP)	245	12/01/2024	12/31/2028

Payment Details

Jan 2024

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 1a	73682	AUTO TAGGING LICENSE	1954	$103,851.93	$0.00	$103,851.93
Year 1a	74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150	$0.00	$0.00	$0.00
Year 1a	BasicLicense	Basic License Bundle	160	$15,939.79	$0.00	$15,939.79
Year 1a	BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	$1,548.63	$72.90	$1,621.53
Year 1a	BWCUwTAP	BWC Unlimited with TAP	1954	$1,026,980.18	$28,894.85	$1,055,875.03
Year 1a	H00001	AB4 Camera Bundle	1954	$0.00	$0.00	$0.00
Year 1a	H00002	AB4 Multi Bay Dock Bundle	245	$0.00	$0.00	$0.00
Year 1a	H00003	AB4 1-Bay Dock Bundle	22	$495.85	$38.43	$534.28
Year 1a	H00004	AB4 FLEX POV HARDWARE BUNDLE	15	$0.00	$0.00	$0.00
Year 1a	ProLicense	Pro License Bundle	50	$12,401.28	$0.00	$12,401.28
Year 1a	T00001	AB4 FLEX POV TAP BUNDLE	15	$597.04	$35.86	$632.90
Invoice Upon Fulfillment	BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	$0.00	$0.00	$0.00
Invoice Upon Fulfillment	T00001	AB4 FLEX POV TAP BUNDLE	15	$0.00	$0.00	$0.00
Total				**$1,161,814.70**	**$29,042.04**	**$1,190,856.74**

Jul 2024

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 1b	73682	AUTO TAGGING LICENSE	1954	$188,161.08	$0.00	$188,161.08
Year 1b	74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150	$0.00	$0.00	$0.00
Year 1b	BasicLicense	Basic License Bundle	160	$28,880.04	$0.00	$28,880.04
Year 1b	BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	$2,805.83	$132.09	$2,937.92
Year 1b	BWCUwTAP	BWC Unlimited with TAP	1954	$1,860,704.01	$52,352.30	$1,913,056.31
Year 1b	H00001	AB4 Camera Bundle	1954	$0.00	$0.00	$0.00
Year 1b	H00002	AB4 Multi Bay Dock Bundle	245	$0.00	$0.00	$0.00
Year 1b	H00003	AB4 1-Bay Dock Bundle	22	$898.40	$69.63	$968.03
Year 1b	H00004	AB4 FLEX POV HARDWARE BUNDLE	15	$0.00	$0.00	$0.00
Year 1b	ProLicense	Pro License Bundle	50	$22,468.92	$0.00	$22,468.92
Year 1b	T00001	AB4 FLEX POV TAP BUNDLE	15	$1,081.72	$64.97	$1,146.69
Total				**$2,105,000.00**	**$52,618.99**	**$2,157,618.99**

Jul 2025

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 2	73682	AUTO TAGGING LICENSE	1954	$203,356.99	$0.00	$203,356.99
Year 2	74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150	$0.00	$0.00	$0.00
Year 2	BasicLicense	Basic License Bundle	160	$31,212.40	$0.00	$31,212.40
Year 2	BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	$3,032.44	$142.75	$3,175.19
Year 2	BWCUwTAP	BWC Unlimited with TAP	1954	$2,010,974.64	$56,580.27	$2,067,554.91
Year 2	H00001	AB4 Camera Bundle	1954	$0.00	$0.00	$0.00

Jul 2025

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 2	H00002	AB4 Multi Bay Dock Bundle	245	$0.00	$0.00	$0.00
Year 2	H00003	AB4 1-Bay Dock Bundle	22	$970.95	$75.25	$1,046.20
Year 2	H00004	AB4 FLEX POV HARDWARE BUNDLE	15	$0.00	$0.00	$0.00
Year 2	ProLicense	Pro License Bundle	50	$24,283.50	$0.00	$24,283.50
Year 2	T00001	AB4 FLEX POV TAP BUNDLE	15	$1,169.08	$70.21	$1,239.29
Total				**$2,275,000.00**	**$56,868.48**	**$2,331,868.48**

Jul 2026

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 3	73682	AUTO TAGGING LICENSE	1954	$210,061.06	$0.00	$210,061.06
Year 3	74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150	$0.00	$0.00	$0.00
Year 3	BasicLicense	Basic License Bundle	160	$32,241.37	$0.00	$32,241.37
Year 3	BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	$3,132.40	$147.46	$3,279.86
Year 3	BWCUwTAP	BWC Unlimited with TAP	1954	$2,077,270.54	$58,445.56	$2,135,716.10
Year 3	H00001	AB4 Camera Bundle	1954	$0.00	$0.00	$0.00
Year 3	H00002	AB4 Multi Bay Dock Bundle	245	$0.00	$0.00	$0.00
Year 3	H00003	AB4 1-Bay Dock Bundle	22	$1,002.96	$77.73	$1,080.69
Year 3	H00004	AB4 FLEX POV HARDWARE BUNDLE	15	$0.00	$0.00	$0.00
Year 3	ProLicense	Pro License Bundle	50	$25,084.06	$0.00	$25,084.06
Year 3	T00001	AB4 FLEX POV TAP BUNDLE	15	$1,207.61	$72.53	$1,280.14
Total				**$2,350,000.00**	**$58,743.28**	**$2,408,743.28**

Jul 2027

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 4	73682	AUTO TAGGING LICENSE	1954	$213,189.63	$0.00	$213,189.63
Year 4	74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150	$0.00	$0.00	$0.00
Year 4	BasicLicense	Basic License Bundle	160	$32,721.57	$0.00	$32,721.57
Year 4	BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	$3,179.05	$149.66	$3,328.71
Year 4	BWCUwTAP	BWC Unlimited with TAP	1954	$2,108,208.60	$59,316.03	$2,167,524.63
Year 4	H00001	AB4 Camera Bundle	1954	$0.00	$0.00	$0.00
Year 4	H00002	AB4 Multi Bay Dock Bundle	245	$0.00	$0.00	$0.00
Year 4	H00003	AB4 1-Bay Dock Bundle	22	$1,017.90	$78.89	$1,096.79
Year 4	H00004	AB4 FLEX POV HARDWARE BUNDLE	15	$0.00	$0.00	$0.00
Year 4	ProLicense	Pro License Bundle	50	$25,457.65	$0.00	$25,457.65
Year 4	T00001	AB4 FLEX POV TAP BUNDLE	15	$1,225.60	$73.61	$1,299.21
Total				**$2,385,000.00**	**$59,618.19**	**$2,444,618.19**

Jul 2028

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 5	73682	AUTO TAGGING LICENSE	1954	$136,539.31	$0.00	$136,539.31

Jul 2028						
Invoice Plan	**Item**	**Description**	**Qty**	**Subtotal**	**Tax**	**Total**
Year 5	74020	MAGNET MOUNT, FLEXIBLE, AXON RAPIDLOCK	2150	$0.00	$0.00	$0.00
Year 5	BasicLicense	Basic License Bundle	160	$20,956.83	$0.00	$20,956.83
Year 5	BWCamSBDTAP	Body Worn Camera Single-Bay Dock TAP Bundle	22	$2,036.05	$95.87	$2,131.92
Year 5	BWCUwTAP	BWC Unlimited with TAP	1954	$1,350,222.05	$37,989.55	$1,388,211.60
Year 5	H00001	AB4 Camera Bundle	1954	$0.00	$0.00	$0.00
Year 5	H00002	AB4 Multi Bay Dock Bundle	245	$0.00	$0.00	$0.00
Year 5	H00003	AB4 1-Bay Dock Bundle	22	$651.92	$50.52	$702.44
Year 5	H00004	AB4 FLEX POV HARDWARE BUNDLE	15	$0.00	$0.00	$0.00
Year 5	ProLicense	Pro License Bundle	50	$16,304.59	$0.00	$16,304.59
Year 5	T00001	AB4 FLEX POV TAP BUNDLE	15	$784.95	$47.13	$832.08
Total				**$1,527,495.70**	**$38,183.07**	**$1,565,678.77**

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.

Standard Terms and Conditions

Axon Enterprise Inc. Sales Terms and Conditions

Axon Master Services and Purchasing Agreement:

This Quote is limited to and conditional upon your acceptance of the provisions set forth herein and Axon's Master Services and Purchasing Agreement (posted at www.axon.com/legal/sales-terms-and-conditions), as well as the attached Statement of Work (SOW) for Axon Fleet and/or Axon Interview Room purchase, if applicable. In the event you and Axon have entered into a prior agreement to govern all future purchases, that agreement shall govern to the extent it includes the products and services being purchased and does not conflict with the Axon Customer Experience Improvement Program Appendix as described below.

ACEIP:

The Axon Customer Experience Improvement Program Appendix, which includes the sharing of de-identified segments of Agency Content with Axon to develop new products and improve your product experience (posted at www.axon.com/legal/sales-terms-and-conditions), is incorporated herein by reference. By signing below, you agree to the terms of the Axon Customer Experience Improvement Program.

Acceptance of Terms:

Any purchase order issued in response to this Quote is subject solely to the above referenced terms and conditions. By signing below, you represent that you are lawfully able to enter into contracts. If you are signing on behalf of an entity (including but not limited to the company, municipality, or government agency for whom you work), you represent to Axon that you have legal authority to bind that entity. If you do not have this authority, please do not sign this Quote.

Signature

Date Signed

11/21/2023



Criminal Justice Information Services (CJIS) Security Policy

Version 5.9
06/01/2020

CJISD-ITS-DOC-08140-5.9

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs 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 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 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 by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and 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 justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving 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 uniform 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 CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

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 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 CJIS Security Policy provides a secure framework of 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
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council
5.9	Incorporate Calendar Year 2019 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2020	APB & Compact Council

SUMMARY OF CHANGES

Version 5.9

APB Approved Changes

1. **Section 5.13.2 Mobile Device Management (MDM)**: add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the *CJIS Security Policy*.
2. **Appendix H, Security Addendum**: add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).
3. **NOTE**: There were no Spring 2019 APB actions.

Administrative Changes[1]

1. **Section 5.6.2.2.2 Advanced Authentication Decision Tree**: updated the tree description to account for direct and indirect access to CJI.
2. **Figures 9 and 10:** updated both figures to account for direct and indirect access to CJI.

KEY TO APB APPROVED CHANGES (e.g. "Fall 2013, APB#11, SA#6, add language, Future CSP for Mobile Devices"):

Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Summary of change

Topic title

[1] Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

TABLE OF CONTENTS

Executive Summary ..... **i**
Change Management ..... **ii**
Summary of Changes ..... **iii**
Table of Contents ..... **iv**
List of Figures ..... **ix**
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 2
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 Government Agency (CGA) 7
3.2.7 Agency Coordinator (AC) 7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO) 7
3.2.9 Local Agency Security Officer (LASO) 8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO) 8
3.2.11 Repository Manager 9
3.2.12 Compact Officer 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
5.1.1.1 Information Handling 15
5.1.1.2 State and Federal Agency User Agreements 15
5.1.1.3 Criminal Justice Agency User Agreements 16
5.1.1.4 Interagency and Management Control Agreements 16
5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 16
5.1.1.6 Agency User Agreements 17
5.1.1.7 Outsourcing Standards for Channelers 17
5.1.1.8 Outsourcing Standards for Non-Channelers 18
5.1.2 Monitoring, Review, and Delivery of Services 18
5.1.2.1 Managing Changes to Service Providers 18
5.1.3 Secondary Dissemination 18
5.1.4 Secondary Dissemination of Non-CHRI CJI 18
5.2 Policy Area 2: Security Awareness Training 20
5.2.1 Basic Security Awareness Training 20
5.2.1.1 Level One Security Awareness Training 20
5.2.1.2 Level Two Security Awareness Training 20
5.2.1.3 Level Three Security Awareness Training 21
5.2.1.4 Level Four Security Awareness Training 21
5.2.2 LASO Training 22
5.2.3 Security Training Records 22
5.3 Policy Area 3: Incident Response 24
5.3.1 Reporting Security Events 24
5.3.1.1 Reporting Structure and Responsibilities 24
5.3.1.1.1 FBI CJIS Division Responsibilities 24
5.3.1.1.2 CSA ISO Responsibilities 24
5.3.2 Management of Security Incidents 25
5.3.2.1 Incident Handling 25
5.3.2.2 Collection of Evidence 25
5.3.3 Incident Response Training 25
5.3.4 Incident Monitoring 25
5.4 Policy Area 4: Auditing and Accountability 27
5.4.1 Auditable Events and Content (Information Systems) 27
5.4.1.1 Events 27
5.4.1.1.1 Content 28
5.4.2 Response to Audit Processing Failures 28
5.4.3 Audit Monitoring, Analysis, and Reporting 28
5.4.4 Time Stamps 28
5.4.5 Protection of Audit Information 28
5.4.6 Audit Record Retention 28
5.4.7 Logging NCIC and III Transactions 29

5.5 Policy Area 5: Access Control 30
5.5.1 Account Management 30
5.5.2 Access Enforcement 30
5.5.2.1 Least Privilege 31
5.5.2.2 System Access Control 31
5.5.2.3 Access Control Criteria 31
5.5.2.4 Access Control Mechanisms 31
5.5.3 Unsuccessful Login Attempts 32
5.5.4 System Use Notification 32
5.5.5 Session Lock 32
5.5.6 Remote Access 33
5.5.6.1 Personally Owned Information Systems 33
5.5.6.2 Publicly Accessible Computers 33
5.6 Policy Area 6: Identification and Authentication 35
5.6.1 Identification Policy and Procedures 35
5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges 35
5.6.2 Authentication Policy and Procedures 35
5.6.2.1 Standard Authenticators 36
5.6.2.1.1 Password 36
5.6.2.1.2 Personal Identification Number (PIN) 38
5.6.2.1.3 One-time Passwords (OTP) 38
5.6.2.2 Advanced Authentication 38
5.6.2.2.1 Advanced Authentication Policy and Rationale 39
5.6.2.2.2 Advanced Authentication Decision Tree 39
5.6.3 Identifier and Authenticator Management 41
5.6.3.1 Identifier Management 41
5.6.3.2 Authenticator Management 42
5.6.4 Assertions 42
5.7 Policy Area 7: Configuration Management 48
5.7.1 Access Restrictions for Changes 48
5.7.1.1 Least Functionality 48
5.7.1.2 Network Diagram 48
5.7.2 Security of Configuration Documentation 48
5.8 Policy Area 8: Media Protection 49
5.8.1 Media Storage and Access 49
5.8.2 Media Transport 49
5.8.2.1 Digital Media during Transport 49
5.8.2.2 Physical Media in Transit 49
5.8.3 Digital Media Sanitization and Disposal 49
5.8.4 Disposal of Physical Media 49
5.9 Policy Area 9: Physical Protection 51
5.9.1 Physically Secure Location 51
5.9.1.1 Security Perimeter 51
5.9.1.2 Physical Access Authorizations 51
5.9.1.3 Physical Access Control 51

5.9.1.4 Access Control for Transmission Medium 51
5.9.1.5 Access Control for Display Medium 51
5.9.1.6 Monitoring Physical Access 52
5.9.1.7 Visitor Control 52
5.9.1.8 Delivery and Removal 52
5.9.2 Controlled Area 52
5.10 Policy Area 10: System and Communications Protection and Information Integrity 53
5.10.1 Information Flow Enforcement 53
5.10.1.1 Boundary Protection 53
5.10.1.2 Encryption 54
5.10.1.2.1 Encryption for CJI in Transit 54
5.10.1.2.2 Encryption for CJI at Rest 55
5.10.1.2.3 Public Key Infrastructure (PKI) Technology 55
5.10.1.3 Intrusion Detection Tools and Techniques 55
5.10.1.4 Voice over Internet Protocol 56
5.10.1.5 Cloud Computing 56
5.10.2 Facsimile Transmission of CJI 57
5.10.3 Partitioning and Virtualization 57
5.10.3.1 Partitioning 57
5.10.3.2 Virtualization 58
5.10.4 System and Information Integrity Policy and Procedures 58
5.10.4.1 Patch Management 58
5.10.4.2 Malicious Code Protection 59
5.10.4.3 Spam and Spyware Protection 59
5.10.4.4 Security Alerts and Advisories 59
5.10.4.5 Information Input Restrictions 60
5.11 Policy Area 11: Formal Audits 61
5.11.1 Audits by the FBI CJIS Division 61
5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division 61
5.11.1.2 Triennial Security Audits by the FBI CJIS Division 61
5.11.2 Audits by the CSA 61
5.11.3 Special Security Inquiries and Audits 62
5.11.4 Compliance Subcommittees 62
5.12 Policy Area 12: Personnel Security 63
5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI 63
5.12.2 Personnel Termination 64
5.12.3 Personnel Transfer 64
5.12.4 Personnel Sanctions 64
5.13 Policy Area 13: Mobile Devices 66
5.13.1 Wireless Communications Technologies 66
5.13.1.1 802.11 Wireless Protocols 66
5.13.1.2 Cellular Devices 67
5.13.1.2.1 Cellular Service Abroad 68
5.13.1.2.2 Voice Transmissions Over Cellular Devices 68
5.13.1.3 Bluetooth 68

5.13.1.4 Mobile Hotspots 68
5.13.2 Mobile Device Management (MDM) 69
5.13.3 Wireless Device Risk Mitigations 69
5.13.4 System Integrity 70
5.13.4.1 Patching/Updates 70
5.13.4.2 Malicious Code Protection 70
5.13.4.3 Personal Firewall 70
5.13.5 Incident Response 71
5.13.6 Access Control 71
5.13.7 Identification and Authentication 71
5.13.7.1 Local Device Authentication 71
5.13.7.2 Advanced Authentication 72
5.13.7.2.1 Compensating Controls 72
5.13.7.3 Device Certificates 72
Appendices A-1
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
D.2 Management Control Agreement D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding D-10
D.4 Interagency Connection Agreement D-16
Appendix E Security Forums and Organizational Entities E-1
Appendix F Sample Forms F-1
F.1 Security Incident Response Form F-2
Appendix G Best practices G-1
G.1 Virtualization G-1
G.2 Voice over Internet Protocol G-4
G.3 Cloud Computing G-15
G.4 Mobile Appendix G-32
G.5 Administrator Accounts for Least Privilege and Separation of Duties G-53
G.6 Encryption G-66
G.7 Incident Response G-76
G.8 Secure Coding G-89
Appendix H Security Addendum H-1
Appendix I References I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance J-1
Appendix K Criminal Justice Agency Supplemental Guidance K-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....19
Figure 4 – Security Awareness Training Use Cases....22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department....26
Figure 6 – Local Police Department's Use of Audit Logs....29
Figure 7 – A Local Police Department's Access Controls....34
Figure 8 – Advanced Authentication Use Cases....42
Figure 9 – Authentication Decision for Known Location....46
Figure 10 – Authentication Decision for Unknown Location....47
Figure 11 – A Local Police Department's Configuration Management Controls....48
Figure 12 – A Local Police Department's Media Management Policies....50
Figure 13 – A Local Police Department's Physical Protection Measures....52
Figure 14 – System and Communications Protection and Information Integrity Use Cases....60
Figure 15 – The Audit of a Local Police Department....62
Figure 16 – A Local Police Department's Personnel Security Controls....64

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 CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) 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). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data 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 CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy 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 CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

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.
- 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.
- References/Citations/Directives: Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

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

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy 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

Every "shall" statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. 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 federal, state, local, and tribal law enforcement 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 represents federal, state, local, and tribal law enforcement and criminal 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 CJIS Security Policy 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.

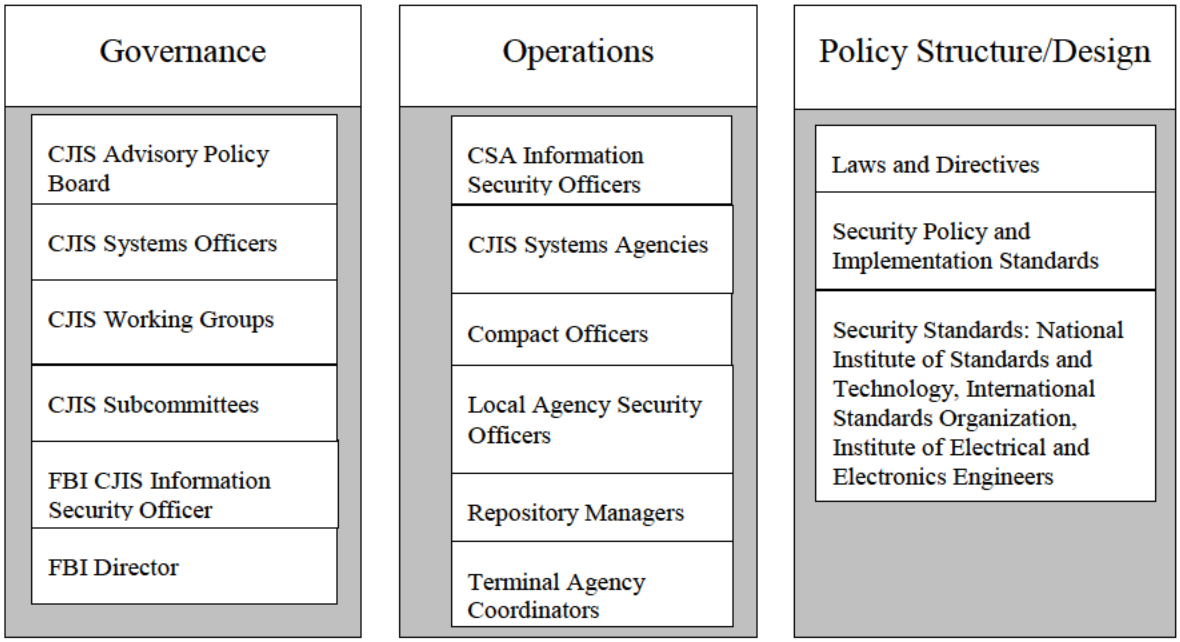


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

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 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, confidentiality, integrity, and availability of service needed by the criminal justice community.
    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 Local Agency Security Officer (LASO).

f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).

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. Outsourcing of Criminal Justice Functions

a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.

b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

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 Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA 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. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
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 Local Agency Security Officer (LASO)

Each LASO 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 Compact Officer

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. Known or Appropriately Suspected Terrorist 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 Known or Appropriately Suspected Terrorist 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 a known or appropriately suspected terrorist.

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:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—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.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. 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:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

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, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is 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 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 CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

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, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, 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. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, 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. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or 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 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.

5.1.1.8 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.

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.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI 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.

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.

5.2 Policy Area 2: Security Awareness Training

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.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness 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 security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. 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 - Level One Security Awareness Training

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 baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness 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 CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness 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 baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness 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 baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – 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.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful 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. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;

b. modify the audit log file;

c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

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.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is 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 may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. 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. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department's Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA's CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client's executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

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 P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

5.6.2.1.1.1 Basic Password Standards

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.1.2 Advanced Password Standards

When agencies elect to follow the advanced password standards, passwords shall:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

a. Passwords obtained from previous breach corpuses

b. Dictionary words

c. Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)

d. Context-specific words, such as the name of the service, the username, and derivatives thereof

4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the “banned passwords” list.
5. If the chosen password is found to be part of a “banned passwords” list, the Verifier shall:
   a. Advise the subscriber that they need to select a different password,
   b. Provide the reason for rejection, and
   c. Require the subscriber to choose a different password.
6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
   a. The salt shall be at least 32 bits in length.
   b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

   Note: 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.
10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
    a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as

network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to "activate" that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Is the access to CJI direct access or indirect access?
    a. If access is direct, proceed to question 2.
    b. If access is indirect, decision tree is completed. AA is not required.
2. Can request's physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3.

a. The IP address is attributed to a physical structure; or

b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is "no". Skip to question number 5.

3. Does request originate from within a physically secure location as described in Section 5.9.1?

   If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 4.

   a. The IP address is attributed to a physically secure location; or

   b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

4. Are all required technical controls implemented at this location or at the controlling agency?

   If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA is not required.

   a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or

   b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

5. Does request originate from an agency-controlled user device?

   If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 6.

   a. The static IP address or MAC address can be traced to registered device; or

   b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

6. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is "yes". Proceed to Figure 9 Step 4.

a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or

b. The certificate presented is associated with a device associated with a criminal justice conveyance; or

c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is "no". Proceed to question number 7.

7. Is the user device an agency-issued and controlled smartphone or tablet?

   If both (a) and (b) below are true, the answer to the above question is "yes." Proceed to question number 8.

   a. The law enforcement agency issued the device to an individual; and

   b. The device is subject to administrative management control of the issuing agency.

   If either (a) or (b) above is false, then the answer is "no." Decision tree completed. AA required.

8. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

   If (a) and (b) below are true, the answer to the above question is "yes." Decision tree completed. AA is not required.

   a. An agency cannot meet a requirement due to legitimate technical or business constraints; and

   b. The CSO has given written approval permitting temporary AA compensating controls to be implemented in lieu of the required AA control measures.

   If either (a) or (b) above is false then the answer is "no." Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.

5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password ("something you know"). Once prompted, the user connects the smart card ("something you have") to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user's agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP ("something you have") then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a one-time password (OTP) is sent to the user's agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user's identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user, is not listed under the user's profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user and is not listed under the user's profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user's profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. Using this collected data, the RBA presents challenge/response questions when changes to the user's profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user's job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device

2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

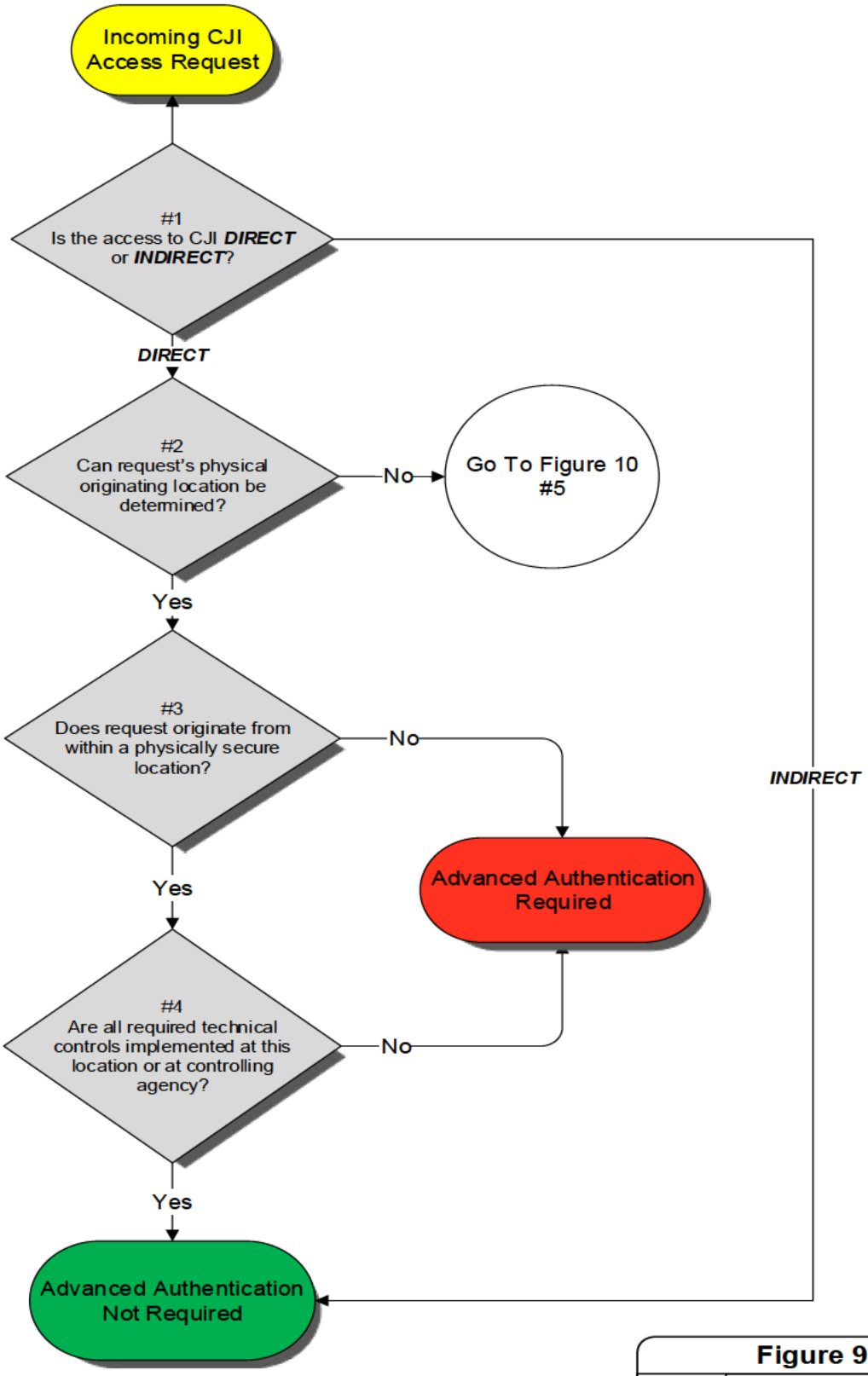


Figure 9
06/01/2020

Figure 10 – Authentication Decision for Unknown Location

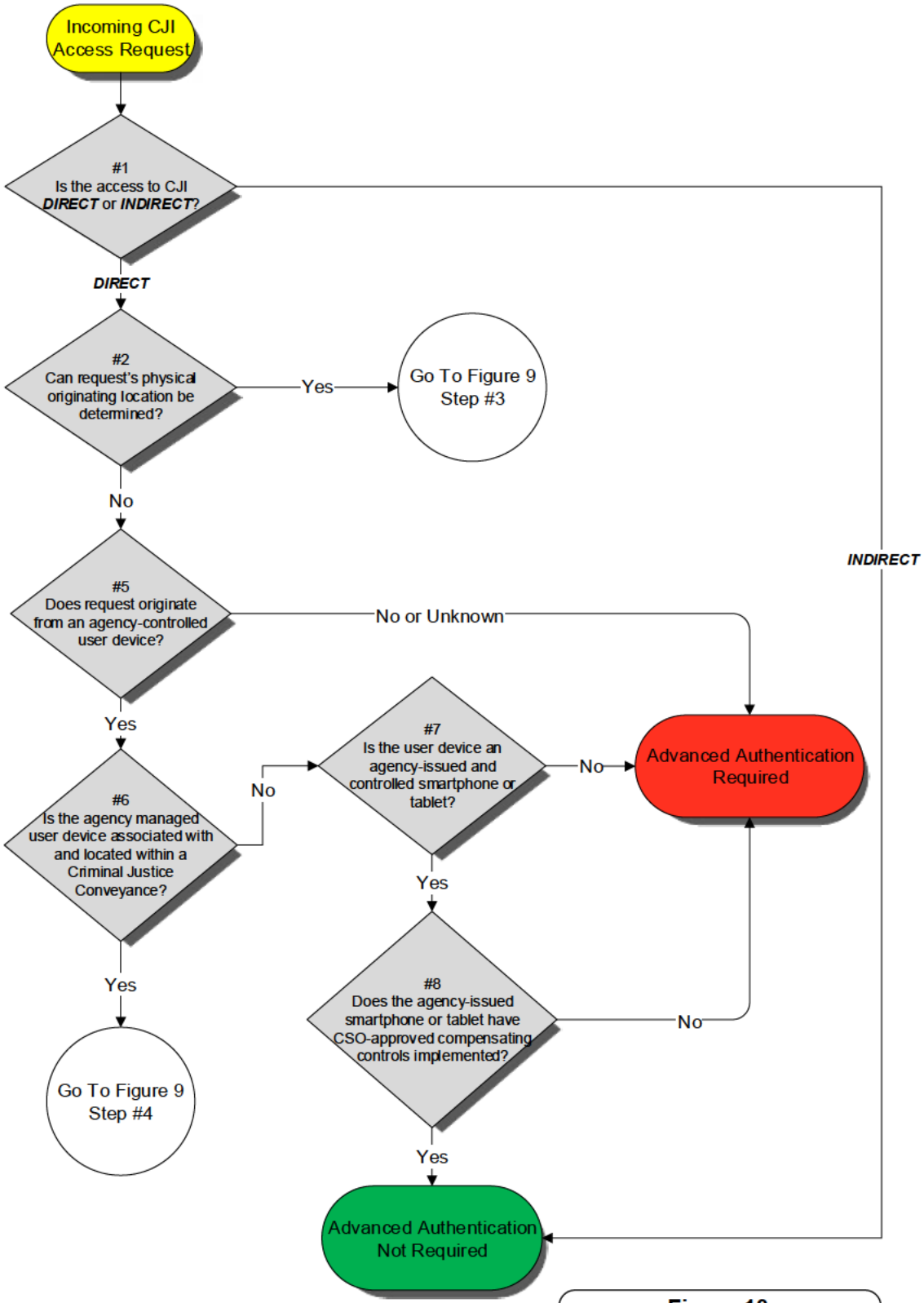


Figure 10
06/01/2020

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. "For Official Use Only" (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – 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.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

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.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is 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. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled 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 Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

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 policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
    a. The agency owns, operates, manages, or protects the medium.
    b. Medium terminates within physically secure locations at both ends with no interconnections between.
    c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
    d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
    e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA) – If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
    a. Be at least 10 characters
    b. Not be a dictionary word.
    c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
    d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

    NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and

monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

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 lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

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. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

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 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 Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

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.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP 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: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

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 including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. 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.

    Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

    See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.

    a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO 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, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.

    c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA 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 or his/her designee 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. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee 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 granting 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.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – 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.

5.13 Policy Area 13: 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.

5.13.1 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.

5.13.1.1 802.11 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 Section 5.6.2.1.
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.

5.13.1.2 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.

5.13.1.2.1 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.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 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.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi 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 Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 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.

5.13.3 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 Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) 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.

5.13.4 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.

5.13.4.1 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.

5.13.4.2 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.

5.13.4.3 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.

5.13.5 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

5.13.6 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.

5.13.7 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.

5.13.7.1 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 section 5.6.2.1 Standard Authenticators.

5.13.7.2 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 Section 5.6.2.2.1. If access is indirect, then AA is not required.

5.13.7.2.1 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 5.13.2. 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 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.13.7.3 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

APPENDIX A TERMS AND DEFINITIONS

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.

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 — (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.

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.

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.

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 Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

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.

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.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

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.

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.

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 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.

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.

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 legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

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.

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, WiFi, 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 (WiFi) Hotspot — A mobile (WiFi) 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.

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.

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.

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.

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.

Property Data — Information about vehicles and property associated with a crime.

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.

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).

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.

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 (WiFi) Hotspot – A wireless (WiFi) 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
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
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
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
TLS	Transport Layer Security
UCN	Universal Control Number
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

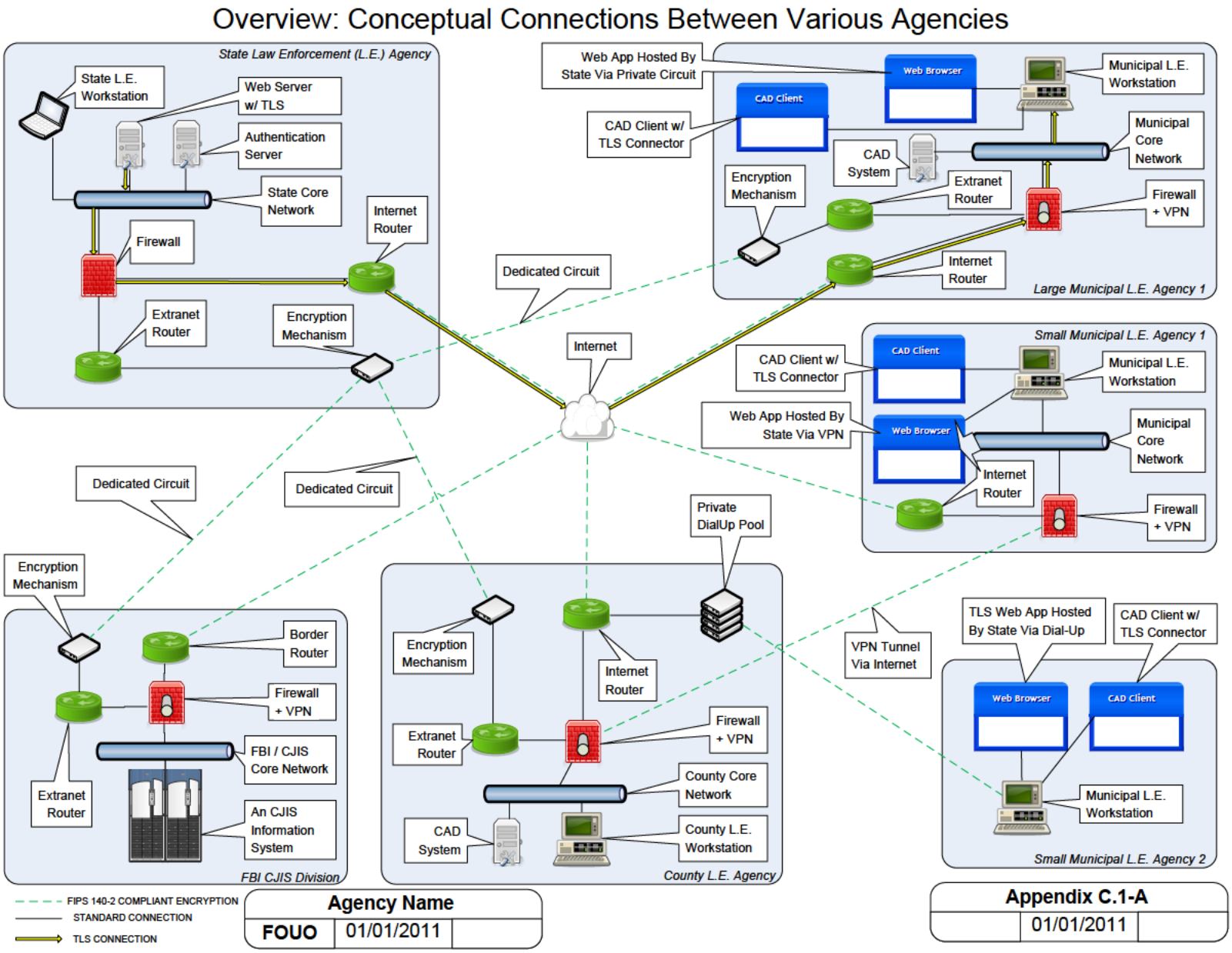


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

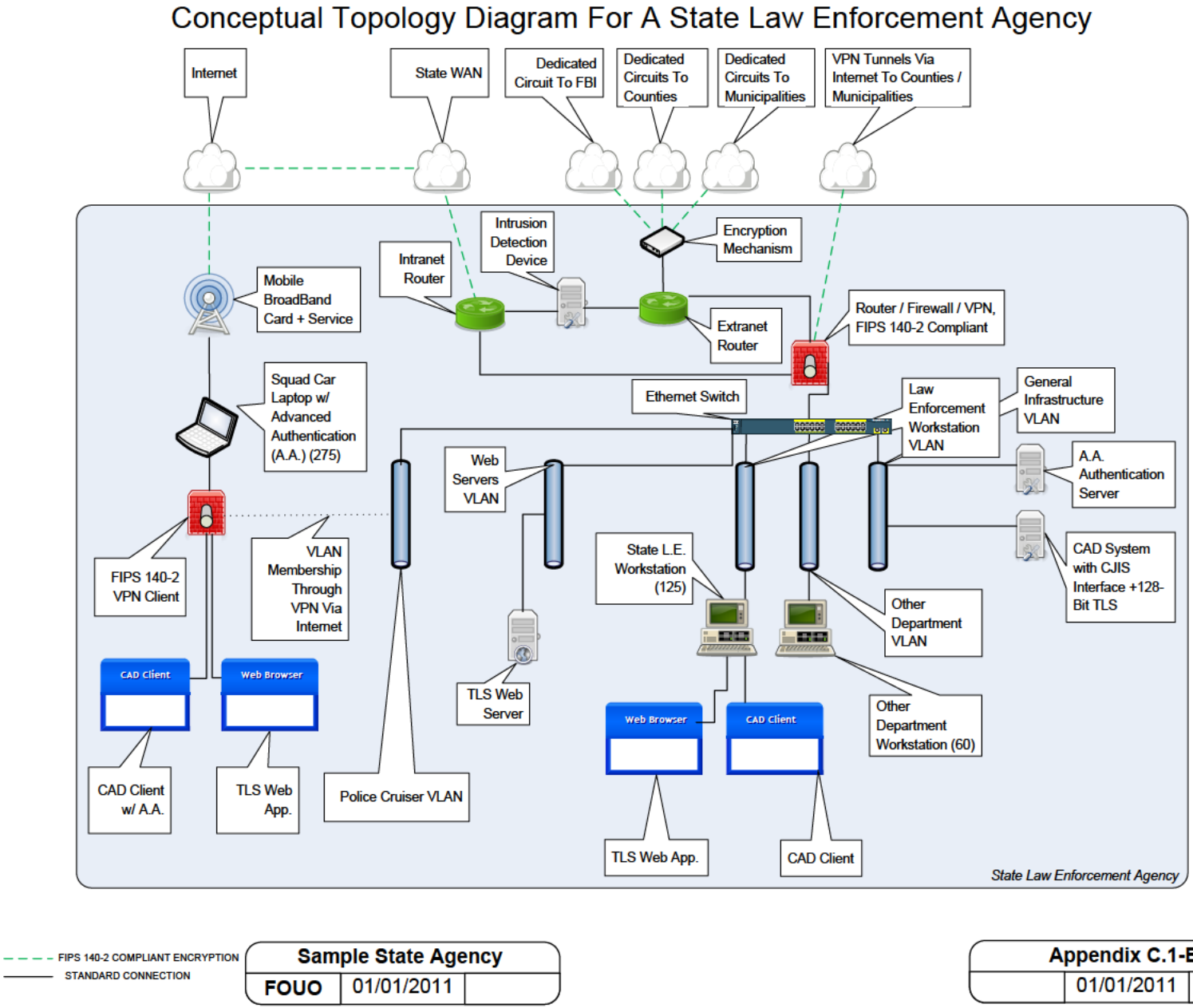


Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

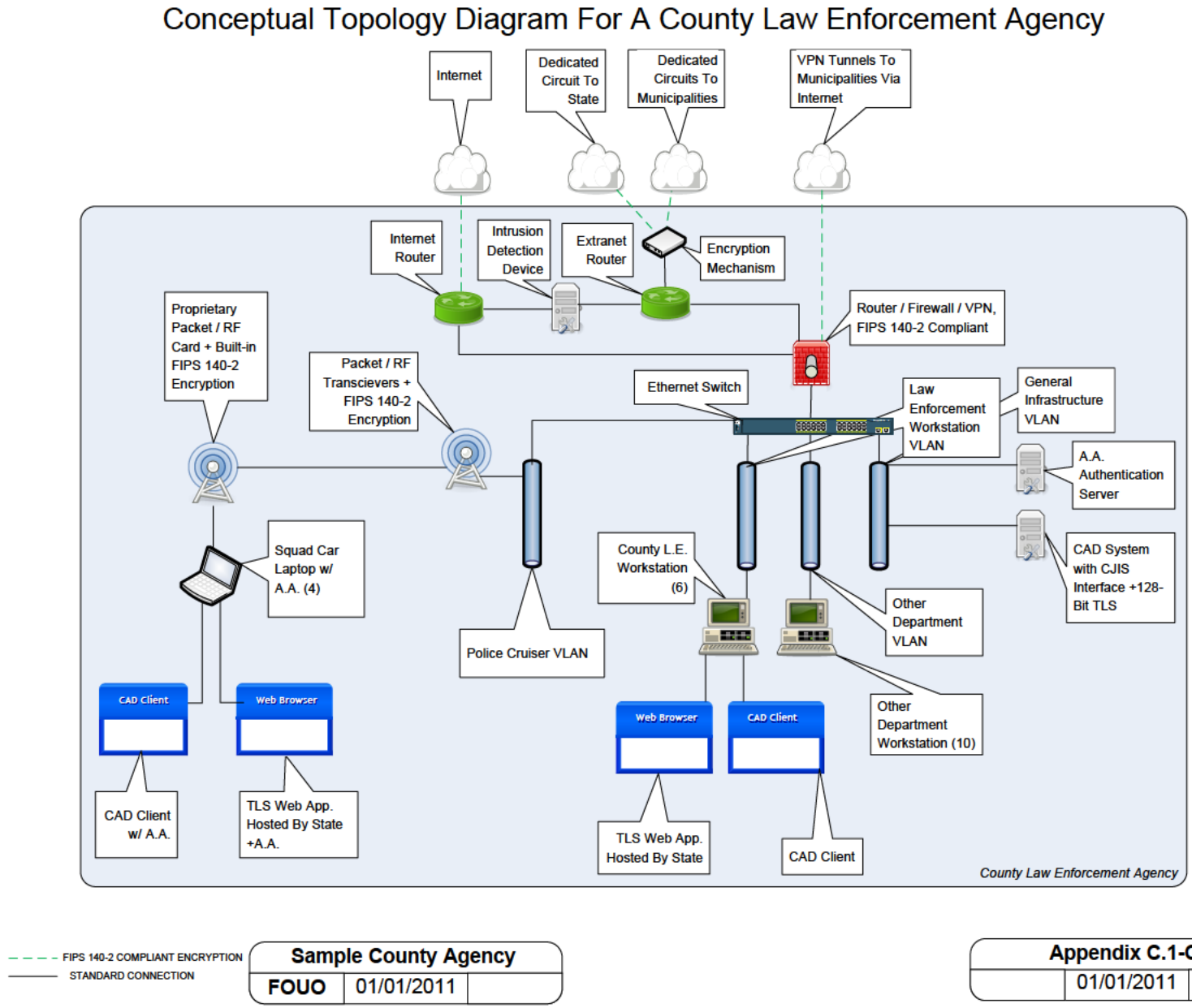
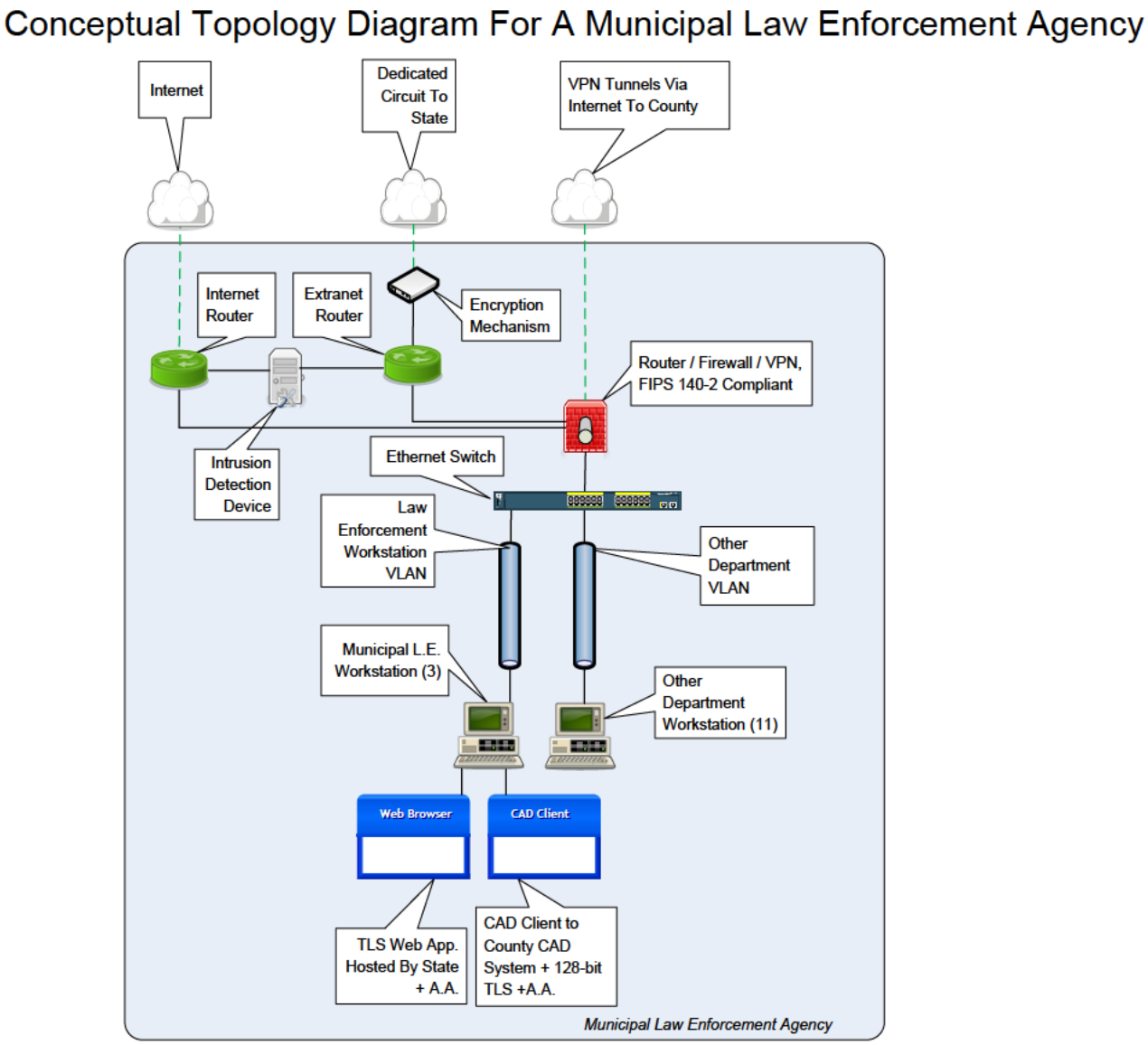


Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency



Sample Municipal Agency		
FOUO	01/01/2011	

Appendix C.1-D		
	01/01/2011	

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.

2. Telecommunication lines to state, federal, and regulatory interfaces.

3. Legal and legislative review of matters pertaining to all CJIS Systems.

4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.

5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.

6. Ongoing assistance to Systems' users through meetings and briefings with the CSO**s**, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.

7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.

9. Annual NICS Users Conference.

10. Audit.

11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.

2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.

3. Biannual file synchronization of information entered into the III by participating states.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.

6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.

7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.

2. CJIS Security Policy.

3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.

4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.

5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.

6. The National Fingerprint File Qualification Requirements.

7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.

8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.

10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.

2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.

3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.

4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.

2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.

3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.

4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.

2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.

3. Either party may terminate this 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 agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), 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 Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy 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 agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both 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 both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity**.** Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

_____ Date: _____

CJIS Systems Officer

_____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

_____ Date: _____

CSA Head

_____

Printed Name/Title

PART 2

_____ Date: _____

CJIS WAN Official (or other CJIS Authorized Official)

_____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

_____ Date: _____

CJIS WAN Agency Head

_____

Printed Name/Title

FBI CJIS DIVISION:

_____ Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

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. $(ISC)^2$
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

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:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi 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 WiFi 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.

8. 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.

   a. Scenario 1–Agency Stores CJI in a Cloud:
      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[2] 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.

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.

[2] 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 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:

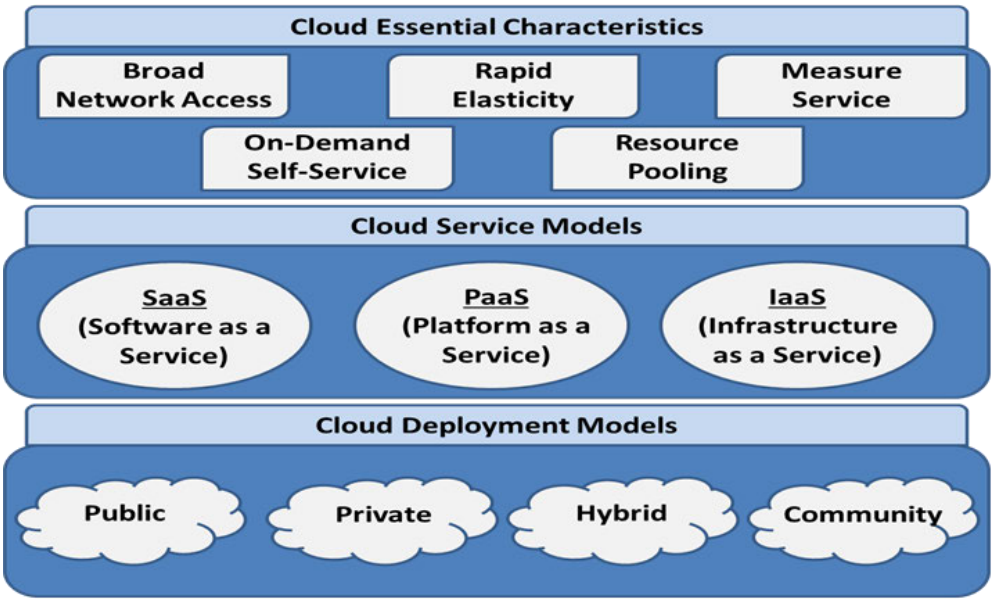


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

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:

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.*

Governance

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.

<u>Availability</u>

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.
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, WiFi + Cellular, WiFi 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 WiFi 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 WiFi 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 WiFi).

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. WiFi 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), WiFi Only (includes 'on demand' cellular), and Cellular (always on) + WiFi 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.

WiFi only (includes ‘on-demand’ cellular)

WiFi 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 WiFi 'hotspots' or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi 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 WiFi 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 WiFi 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' WiFi 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 WiFi access points.

WiFi 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) + WiFi 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 WiFi 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 WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi 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 WiFi 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 WiFi 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, WiFi, 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 WiFi Policy

Specific WiFi 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 WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (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 WiFi 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 WiFi 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 WiFi 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 WiFi 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 WiFi 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 WiFi 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).

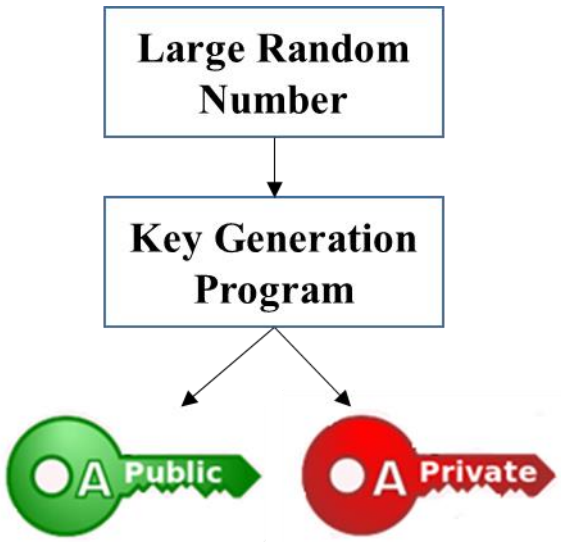


Figure 1 – Asymmetric key pair generation

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

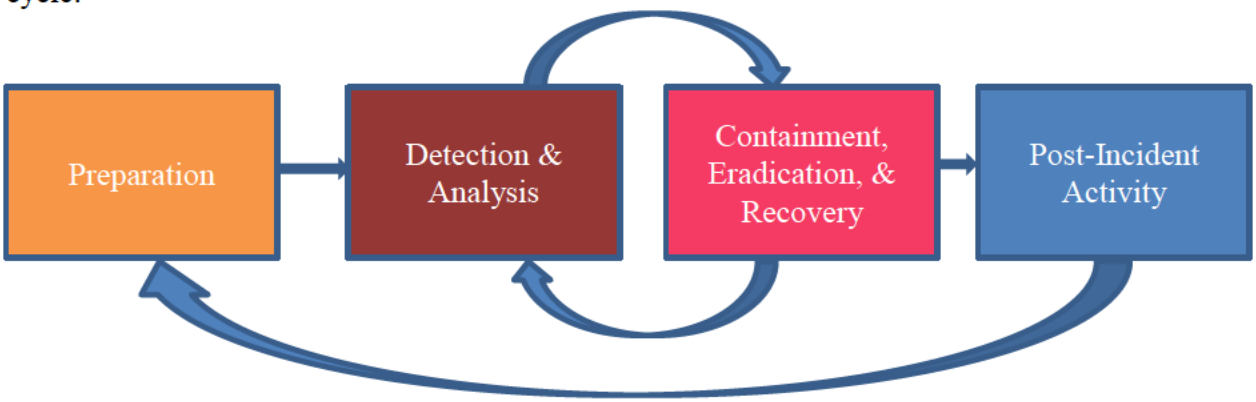
Introduction

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:



Preparation

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

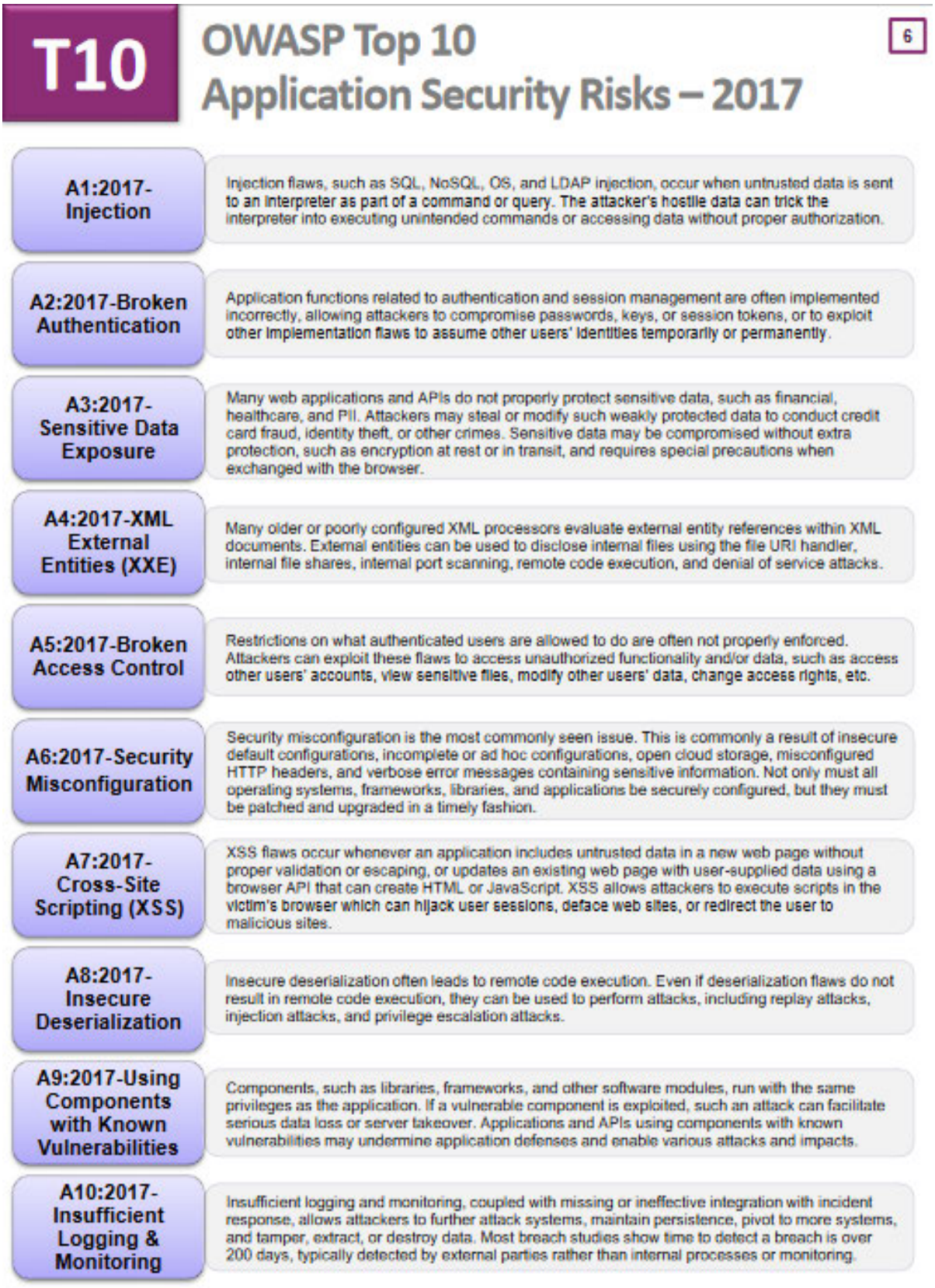
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

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.

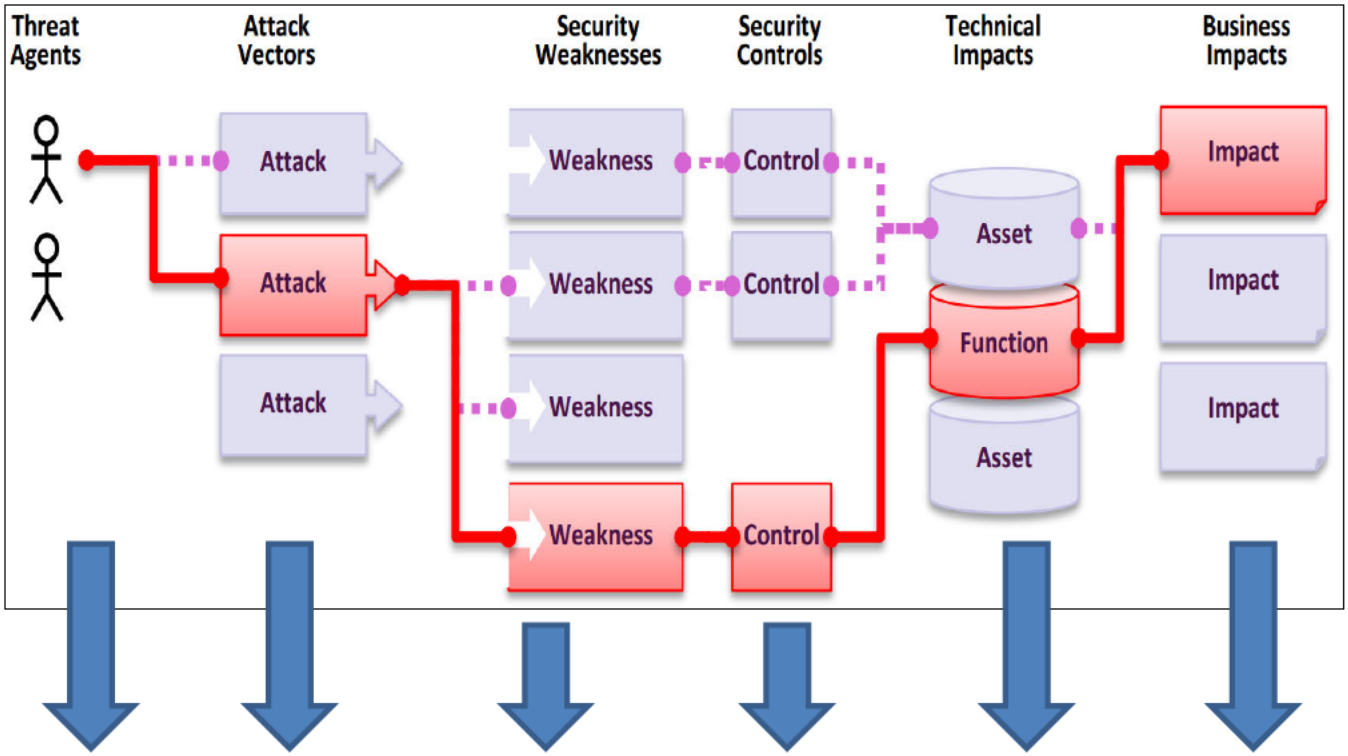
Application Security Risks

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: Exploitability	Security Weakness: Prevalence	Security Weakness: Detectability	Impacts: Technical	Impacts: Business	Score
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 (H2-H4);

An example of a contract addendum (H-5);

The Security Addendum itself (H6-H7);

The Security Addendum Certification page (H8).

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]: _____

[Name]

_____

[Title]

_____

Date

On behalf of [Party No. 2]: _____

[Name]

_____

[Title]

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 Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2

[NIST SP 800–53A] *Guide for Assessing the Security Controls 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

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and 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 justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI*)* it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific "shall" statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who 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 (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

(i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,

(ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative

to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

"Electronic media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn't possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, 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. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data "at rest") of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record

information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. 5.5 – Access Control

   CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

   CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

   CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

   CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

   CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

   CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as "terminal agencies".

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and 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 justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific "shall" statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who 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 (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

(iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,

(iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

"Digital media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn't possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, 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. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data "at rest") of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency's virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above "General CJI Guidance" section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the "General CJI Guidance", focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the "General CJI Guidance", focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this

situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the "General CJI Guidance", focus on compliance with policy sections:

a. 5.5 – Access Control

   CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

   CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

   CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

   CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

   CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

   CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

   A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

   Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

   NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

   A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

   To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

   NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

TAB B - EXECUTIVE SUMMARY AND RESPONSES TO SPECIFICATIONS

This section includes an executive summary and Axon's responses to the City's specifications.

The following one-page executive summary provides a high-level description of Axon's ability to meet the requirements of the RFP and the reasons we believe we are best qualified to provide the identified services.

EXECUTIVE SUMMARY

Since 2014, San Diego Police Department (SDPD) has worked with Axon Enterprise, Inc. (Axon) to roll out, deploy, and maintain a successful body-worn camera program of more than 2,000 cameras. And, after approximately nine years of using our solution, we hope SDPD's firsthand experience with our cameras has led to improved confidence in safety and transparency in the field, as well as the building of better relations across the communities you serve.

To continue building on our successful working relationship, Axon remains dedicated to supporting your current Axon solutions, while also providing you with more tools as recruits join your force after graduation. This includes continued support for the software and applications you use every day, such as Axon Evidence, Axon Capture, and Axon Citizen (Axon Community Request). These applications have given SDPD secure and expansive storage and evidence collection options that are cost-effective, scalable, and easy to use.

In addition to partnering on SDPD's body-worn camera solution, Axon has also been your TASER energy weapon provider since 2009. With more than 14 years of experience working with your agency, including direct communication with our CEO Rick Smith and Axon's Product Teams. Axon is confident our unique history together will continue to benefit your long team goals. Throughout this history, we have joined forces to:

- Develop the mobile application, Axon Capture, which allows agencies around the world to capture evidence with mobile devices
- Set up workflows to share your evidence with local cities, municipalities, and federal organizations such as the MCRD, FBI, DOJ, and Border Control
- Transition SDPD to a cloud-based evidence collection workflow, Axon Citizen, which reduced your physical storage arrays, including 1,300 fewer discs

By remaining with Axon, not only will SDPD benefit from a vendor that knows and supports your goal of protecting both your officers and the community, but you will also preserve the valuable resources and time it would take to transition to a new vendor's system. With our cameras and software already in place, SDPD can:

- Avoid service disruptions by continuing to deploy reliable and familiar Axon solutions
- Quickly train staff on solutions you have experience using day in, day out
- Continue to save time via established evidence collections and sharing workflows that have the highest level of on-cloud security
- Rely on fast, resolution-focused support from a dedicated customer success manager and 24/7 customer support team
- Easily store third-party data from various sources and unlimited data captured on Axon devices
- Deploy Auto-Tagging capabilities that retroactively add metadata to existing evidence, including activation of body-worn cameras via TASER energy weapons

We look forward to improving our existing partnership with SDPD through innovation and scalability as our technology grows and your needs evolve.

RESPONSE TO SPECIFICATIONS

Axon's responses to the following specifications, broken out by topic as indicated by the RFP.

1. Experience
2. Financials
3. Litigation
4. BWC Specifications
5. Software Technical Specifications:
6. Design Requirements
7. Docking Station Specifications.
8. Video Management/Storage System Specifications
9. Additional Available Features
10. Pricing Schedule
11. Training Requirements
12. Staffing Plan
13. Security And Privacy
14. Subcontractors
15. Delivery
16. Returns
17. Reference checks

1. EXPERIENCE

Briefly, as an overview, Proposer shall describe their experience in providing the goods and services described in this RFP. Proposer shall have a minimum of five (5) years of verifiable experience in delivering and currently maintaining BWC, Video Management, and Storage solutions. Proposers shall provide a list of a minimum of three (3) references of law enforcement agencies where you have provided similar services with at least 1,500 BWCs for each agency.

BODY-WORN CAMERA EXPERIENCE



Axon has spent over a decade manufacturing, delivering, and maintaining BWC, Video Management, and Storage solutions, developed and manufactured multiple generations of body-worn cameras. Since 2012, this includes the Axon Flex 2, Axon Body 2, and Axon Body 3. Axon currently supports our customers' deployment of more than 674,000 registered body-worn cameras worldwide. During this time, our engineers and product managers have expanded our product lines to include first-person point-of-view cameras designed to imitate the human eye, as well as devices equipped with real-time awareness capabilities such as access to livestreams and real-time officer location and alerts.

The Axon platform of connected video recording, cloud, and mobile technologies is built around Axon Evidence, a scalable, cloud-based system that centralizes all types of digital files. Axon Evidence has been operating at scale since 2009.

OUR EXPERIENCE ACROSS THE GLOBE

Axon has supported SDPD with a body-worn camera program of over 2,000 cameras for over eight years, as well as an accompanying evidence application and storage program. To date, the largest purchase of body-worn cameras has been made by the London Metropolitan Police Service in London, UK in the amount of approximately 22,000 devices. In the U.S., the largest purchase of body-worn cameras was made by the Los Angeles Police Department in the amount of approximately 7,500 devices. Axon is responsible for the manufacturing and fulfillment of these orders, including ongoing support for each body-worn camera program after delivery and throughout the life of contracts.

In addition to the SDPD some of Axon's body-worn camera customers include:

- Alameda County, CA SO
- Pasadena, CA PD
- Santa Monica, CA PD
- Chula Vista, CA PD
- Beverly Hills, CA PD
- Dallas, TX PD
- Denver, CO PD
- Atlanta, GA PD
- Fresno, CA PD
- San Jose, CA PD
- Broward County, FL SO
- Fort Worth, TX PD

REFERENCES

1. Company Name: Phoenix Police Department

   Contact Name and Phone Number: Geri Padilla, IT; 602-262-4913

   Contact Email: geri.padilla@phoenix.gov

   Address: 620 W Washington St, Phoenix, AZ 85003

   Contract Date: June 2023 – 5 Year

   Contract Amount: $35,501,131

   Requirements of Contract: Body-worn camera program combined with extensive bundle of Evidence.com features such as Performance, Redaction Assistant, Unlimited 3rd Party storage, and Unlimited Transcription. Deployment of 3,129 body worn cameras and licenses.

2. Company Name: Atlanta Police Department

   Contact Name and Phone Number: Sergeant Paul Bryant, 404-623-3201

   Contact Email: pabryant@atlantaga.gov

   Address: 226 Peachtree St SW Atlanta, GA 30303

   Contract Date: March 2023, 12 Year, Contract Amount: $105,673,922

   Requirements of Contract: Officer Safety Program, combined body-worn camera, Taser, deployment services, storage, licensing, Fleet (in-car cameras), Records (RMS), Interview, and AIR (UAV program) for 2,100 personnel.

3. Company Name: Santa Clara County Sheriff's Office

   Contact Name and Phone Number: Sergeant Ryan Dunn, 408-623-7518

   Contact Email: ryan.dunn@shf.sccgov.org

   Address: 55 West Younger Avenue San Jose, CA 95110

   Contract Date: December 2022, Contract Amount: $15,410,400.00

   Requirements of Contract: 2:1 Body Worn Camera Workflow, 1,275 body-worn cameras, deployment services, storage, and licensing. (Unlimited 7 Premium).

4. Company Name: Los Angeles Police Department

   Contact Name and Phone Number: Robert Bean, Sergeant II, Office: 213-486-0370, Mobile: 213-864-6417

   Contact Email: 37151@lapd.online

   Address: 100 West 1st Street, Suite 842, Los Angeles, CA 90012

   Contract Date: May 2020, Contract Amount: $52,000,000

   Requirements of Contract: 1,500 Fleet Vehicles, 7,255 body-worn cameras, Video Evidence Management, Warranty and Implementation Services

5. Company Name: Los Angeles Sheriff's Department

   Contact Name and Phone Number: Lieutenant Geoffrey Chadwick, Office: (562) 345-2730, Mobile: (213) 238-0751

   Contact Email: gnchadwi@lasd.org

   Address: 12440 Imperial Highway, Norwalk, CA 90650

   Contract Date: August 2020, Contract Amount: $25,610974.00

   Requirements of Contract: 5,248 Body Worn Cameras, Video Evidence Management, Warranty and Implementation Services.

2. FINANCIALS

Proposers shall provide documentation to support your organization's financial stability and ability to maintain the program throughout the contract period.

Axon is a publicly-traded company; all financial information is available at investor.axon.com. Axon's NASDAQ stock ticker symbol is AXON. https://investor.axon.com/financials/sec-filings/default.aspx

FINANCIAL STATEMENTS

Documentation may include cash and/or credit reserves. In addition, the proposer shall provide the following information for the last three (3) fiscal years:

1. **Statement of Financial Position (Balance Sheet);**
2. **Statement of Activities (Income Statement); and**
3. **Statement of Cash Flow**

Appendix 1was uploaded to the portal and the reports can also be accessed using the links below. Axon's financial statements for the past 3 (three) fiscal years are included as one file. Appendix 1 is also included on the USB drive containing our proposal.

2020

2021

2022

3. LITIGATION

Proposer shall provide the status of any lawsuits and/or pending litigation that involve failure to deliver performance on similar scope contracts and/or lawsuits/litigation that directly impact this contract (i.e., technology patents, etc.). Provide information regarding status, resolutions, and if any penalties, fines, or other actions required.

No pending lawsuits/litigation involve Axon's failure to deliver performance on similar scope contracts (i.e., BWC contracts), or involve intellectual property or technology that could directly impact Axon's ability to fulfill its obligations under this contract.

4. BWC SPECIFICATIONS

The proposer must meet the following specifications and requirements:

Axon is responding with two camera models, the Axon Body 3 and the Axon Body 4. The SDPD may select either model and we've included pricing reflective of both options. Where the response differs, we've included a header indicating which response correlates to which camera. In the event that the answer is the same for both models, we've provided one answer which applies to all camera models.

Hardware Technical Specifications:

1. **All BWCs must be factory new with no previous owner. They shall be the latest model in current production or, if multiple models are available, the model chosen by the City.**

Yes. All body-worn cameras supplied will be factory new with no previous owner, shall be the latest model in current production, or the model chosen by the City.

2. **BWC must attach to the chest/upper torso area (patrol and investigations).**

Yes. The image below shows the Axon Body 3 mounted on an officer's torso and on an officer's chest.



The image below shows the Axon Body 4 mounted on an officer's chest. Our versatile mounts also allow for attaching camera to an officer's torso in various configurations, as described in response to question 9 below.



3. Smaller cameras capable of being attached to specialized unit helmets must be available.

Yes. The Action Camera Mount is a GoPro-style mount adapter that allows an Axon Body 3 or Axon Body 4 body-worn camera to be used in a variety of scenarios, including but not limited to, attaching the mount to a helmet using a night vision goggle mount, viewing down tunnels or over walls with a third-party selfie stick, or setting up surveillance on a tripod. This mount is compatible with most GoPro-style third-party action camera mounts, which are sold separately.

AXON BODY 4 POV ACCESSORY

The Flex POV module for Axon Body 4, an optional accessory designed to provide high-quality visual and audio capture, unlocking point-of-view recording capabilities to enhance situational awareness and informed decision-making.

The Flex POV module features unparalleled image and sound quality, capturing clear, high-resolution footage and crisp audio. This makes it an indispensable tool for anyone who needs to quickly and accurately assess a situation and make informed decisions.

With its compact and lightweight design, the Flex POV module is 30% smaller than Flex 2 and does not require recharging. It can be easily connected with the Axon Body 4 in seconds, ensuring hassle-free switching between point-of-view and traditional camera modes.

The module is perfect for use in challenging environments and situations where point-of-view recording provides a unique and invaluable perspective, such as those experienced by SWAT and firearms teams. It also unlocks flexibility for agencies and organizations by eliminating the need to choose between a point of view or a traditional body worn camera. Users can now select the option that makes the most sense for the situation.

4. BWC must be functional in all potential operating temperatures in San Diego County.

Yes. Both the Axon Body 3 and Axon Body 4 cameras have an operating temperature range of -4°–122°F [-20°–50°C]. The cameras can withstand extreme temperatures, which keeps crucial evidence safe and allows officers to rely on the camera's functionality in almost any environment throughout the year.

The high-temperature tolerance proves valuable on particularly warm days when storing a device in a vehicle or when responding to incidents involving excessive heat, such as a residential or car fire.

5. BWC must be functional in relative humidity up to 80% (non-condensing).

Yes. Both the Axon Body 3 and the Axon Body 4 are tested to and pass MIL-STD-810G Test Methods for vibration, salt fog, and blowing dust resistance. The devices operate normally in up to 95% humidity (non-condensing).

6. BWC must have an estimated useful life: Approximately 5 years.

Yes. Both cameras have an approximate useful life of five (5) years. The Axon Technology Assurance Plan (TAP) for Axon body-worn cameras includes Axon's Extended Warranty for the five-year contract term, spare cameras, and camera refreshes for body-worn cameras purchased at the beginning of the contract. Camera refreshes occur twice in the contract term, at the two-and-a-half and five-year marks, free of charge.

7. BWC will have a rechargeable lithium-ion battery or similar capable of lasting at least a working shift of 12 hours on a single charge.

Yes. Both cameras have an internal, rechargeable, lithium-ion polymer battery. Under normal usage (such as during a working shift), the cameras are capable of providing approximately 12 hours of battery life on a single charge.

Some of the advanced functions, such as livestreaming, will result in greater battery consumption and impact battery life during a shift.

8. BWC must have multiple microphones built into the camera for clearer sound.

Yes. Both cameras include four (4) internal microphones.

The Axon Body 3 includes four (4) built-in microphones on different planes of the camera. An audio algorithm developed in partnership with Nokia dramatically improves the audio captured by the Axon Body 3 camera, compared to its predecessor.

This sophisticated onboard audio processing (Nokia Ozo-based) to reduce wind noise, calculates automatic gain control, and other functions to record the clearest stereo recording possible even in dynamic situations.

The Axon Body 4 camera leverages four (4) built-in digital microphones on different planes within the device. With each microphone positioned several centimeters apart, the audio signals received are slightly delayed or phase-shifted. This arrangement is similar to how humans discern the direction of sound using two ears. Built-in algorithms then take advantage of these shifts to produce a binaural (stereo) output stream, and also help prioritize back-and-forth interactions over background noise.

By setting the microphones on different planes, captured evidence also benefits from:

- **IMPROVED OVERALL AUDIO QUALITY AND CLARITY** by capturing and analyzing sounds from multiple angles
- **IMPROVED PERCEPTION** of where sounds are coming from in a video
- **REDUCED ELECTROMAGNETIC INTERFERENCE** to reduce unwanted disturbances

Additionally, the Axon Body 4 camera uses a Nokia OZO-based algorithm that dramatically improves speech intelligibility and reduces unwanted environmental noise. The algorithm's sophisticated onboard audio processing conducts wind noise reduction, calculates automatic gain control, and produces high-quality stereo audio recordings.

The Nokia-OZO-based algorithm also uses the following technology to improve overall audio quality:

- **AUDIO FOCUS** – This algorithm helps accentuate voices while retaining background noises, and prioritizing the camera operator's voice and any sounds coming directly from in front of the operator.
- **AUDIO WINDSCREEN** – This algorithm provides wind noise reduction by leveraging microphones on different planes, which reduces wind noise to allow for a better listening experience and improved chance of hearing voices.
- **AUTOMATIC GAIN CONTROL** – This algorithm helps optimize audio and minimize clipping.

Lastly, Axon applies AAC compression—which is one of the most common compression schemes in use today—to the Nokia OZO output to reduce file size and allow for the storage of more evidence in memory. AAC compression utilizes psychoacoustic compression principles to remove imperceptible portions of an audio stream. By using a setting of 128kbps (nominal), the evidence files captured by the Axon Body 4 camera produce a high-quality output.

AUDIO OUTPUT DETAILS

The Axon Body 4 camera has a sampling rate of 48kHz that allows for the capture of up to 24khz, which is above the human hearing threshold. The camera also has a minimum audio resolution bit depth of 16 bits and utilizes AAC compression, all of which are widely used in the audio industry.

9. BWC must be available with a variety of mounts to attach to uniforms or other equipment including MOLLE mounts.

Yes. Axon offers a variety of mounts made specifically to attach to a uniform and other law enforcement equipment, such as tactical vests, heavy outerwear, duty belts, shirt uniforms, pockets, helmets and more. All mounts described below are available for both the Axon Body 3 and the Axon Body 4.

We offer three Molle mounts, described below.

MOLLE MOUNTS



- **THE MINI MOLLE MOUNT** is a smaller version of the Axon Single Molle mount. Axon has worked closely with Blauer Manufacturing, a leading supplier of law enforcement uniforms, to ensure the Mini Molle has an exact fit with their sew-on nylon Molle loop.

- **THE SINGLE MOLLE MOUNT** is compatible with uniforms that include Molle loops or straps. This mount is durable and easy-to-install on any portion of a uniform that includes Molle straps offers a high-retention-force camera mount solution.
- **THE DOUBLE MOLLE MOUNT** is a slightly larger, studier version of the single Molle mount. Compatible with uniforms that include Molle loops or straps, this mount is durable and easy-to-install on any portion of a uniform that includes Molle straps and offers a high-retention-force camera mount solution.

Generally speaking, molle mounts are considered "high retention" because they are not likely to be detached from their mounting location. This makes them most useful in applications where the chance of detachment is high—such as in dynamic law enforcement situations. In partnering with different agencies over the years,

OTHER AVAILABLE MOUNTS

Axon has developed many other mounts in addition to the high retention molle mounts, and can make those available to SDPD as well. The rest of our mounting solutions, categorized based on their level of retention, are described in detail below.



LOW RETENTION FORCE

- **THE FLEXIBLE MAGNET MOUNT** is an easy-to-install mount with versatile mounting locations.
- **THE REINFORCED FLEXIBLE MAGNET MOUNT** is the reinforced version of the Flexible Magnet mount that is easy to install, with versatile mounting locations and breakaway options.
- **THE BELT CLIP MOUNT** allows the user to comfortably wear the body-worn camera anywhere on the belt.
- **THE OUTERWEAR MAGNET MOUNT** offers versatile mounting locations and breakaway options. This mount is not recommended for Axon Body 3 cameras with Axon Respond and Axon Respond+ since a large amount of metal may impact LTE performance in areas of low coverage.

MEDIUM RETENTION FORCE

- **THE WING CLIP MOUNT** is easy to install and offers versatile mounting locations.
- **THE VELCRO MOUNT** allows versatile mounting locations when there is existing Velcro on the uniform.
- **THE Z-BRACKET MOUNT (AVAILABLE FOR MEN AND WOMEN UNIFORMS)** allows the body-worn camera to be placed at the center of mass when wearing a buttoned shirt.
- **THE POCKET MOUNT (SMALL 4" OR LARGE 6")** is easy to install in a uniform pocket.
- **THE TILT MOUNT (MEDIUM/HIGH RETENTION FORCE)** has a tilt angle that can be easily adjusted when the camera is attached. This mount must be paired with a primary Rapidlock mount, such as the Wing Clip or Molle mount.

HIGH RETENTION FORCE

- **THE HIGH RETENTION WING CLIP MOUNT** combines the versatility of the original Wing Clip with new design elements that increase the overall retention force
- **THE ANCHOR MOUNT** is an easy-to-install, high-retention-force mount that is designed to support outerwear or ballistic vests that offer versatile mounting locations. This semi-permanent mount is best worn on outerwear or a ballistic vest and requires alteration to the uniform.
- **THE ACTION CAMERA MOUNT** is a GoPro-style mount adapter that allows a body-worn camera to be used in a variety of scenarios, including but not limited to, attaching the mount to a helmet using a night vision goggle mount, viewing down tunnels or over walls with a third-party selfie stick, or setting up surveillance on a tripod. This mount is compatible with most GoPro-style third-party action camera mounts, which are sold separately.
- **THE SLIM MOUNT** is a low-profile and lightweight mount with high retention and a minimal footprint. This mount is ideal for use cases where Wing Clips or Molle Mounts are not feasible due to limited space requirements, but high retention force is necessary.

- **THE PATCH MOUNT** is a reliable and high-retention mounting solution that offers compatibility with an existing vest and chest patch. It is compatible with a 4" tall Velcro patch area.
- **THE JACKET MOUNT** is a non-magnetic mount designed for outerwear and thick fabric uniforms which offers high retention force and versatile placement.
- **THE FOLDING MOUNT** is a high retention, low profile, non-magnetic Rapidlock mount that is simple to install and has versatile placement options. The folding rear component snaps into place in seconds and includes a convenient "push to unlock" button for quick release.

10. BWC must be Bluetooth and Wi-Fi enabled.

Yes. Both the Axon Body 3 and Axon Body 4 utilize Bluetooth Low Energy (BLE) 4.2. Axon cameras feature a Wi-Fi transmitter enabled with 802.11ac/b/g/n at 5 GHz and 2.4 GHz. Axon products are designed to use the most secure forms of wireless technology, while also considering power usage, battery life, and ease-of-use.

11. BWC must have at least 64 GB of internal memory.

Yes. The Axon Body 3 has 64 GB of internal memory. The Axon Body 4 camera has a large on-device storage capacity of 128 GB to house captured video files and the camera's operating system.

12. All BWCs must have a full replacement warranty of at least 1 year.

Yes. Axon's proposal includes a full replacement warranty for the entire life of the five-year term, regardless of the camera model chosen.

13. BWC must have the capability to attach camera accessories fitting a wide range of mounts for special purpose units.

Yes. When it comes to body-worn cameras, ensuring that each user has the proper mount for their job and uniform can make all the difference in helping to ensure the camera is able to record critical digital evidence while not hindering the user. For example, if a user works a desk job and mostly wears button-down shirts with breast pockets, a pocket mount that is easily to slip on and off may be best. A user facing more dynamic situations may want maximum retention force for their mount, or may prefer a "breakaway" mount like an Axon Flexible Magnet Mount, which allows the camera to easily detach so as not to become a holding point for an attacker. Please see the response to question #9 which fully details each mount.

5. SOFTWARE TECHNICAL SPECIFICATIONS:

1. BWC must be a full color audio/video camera.

Yes. Both cameras record full color video and audio.

2. Ability to record in multiple color video resolutions that can be selected by the City.

Yes. The cameras each have four video quality settings. The video resolution, encoding bit rate, frame rate, and video encoding format impact the size of files captured at each setting.

AXON BODY 3

Recording capacity and associated settings are defined below.

- The 480p resolution setting captures video at a rate of 0.9 GB per 60 minutes of video. This setting supports the storage of approximately 46 hours of video.
- The 720p L resolution setting captures video at a rate of 1.2 GB per 60 minutes of video. This setting supports the storage of approximately 38 hours of video.
- The 720p H resolution setting captures video at a rate of 2.0 GB per 60 minutes of video. This setting supports the storage of approximately 25 hours of video.
- The 1080p resolution setting captures video at a rate of 4.5 GB per 60 minutes of video. This supports the storage of approximately 11 hours of video.

Please note, storage capacity is based on ~54 GB of available storage to account for the camera's operating system.

AXON BODY 4

- The 480p resolution setting captures video at a rate of 0.97 GB per 60 minutes of video. This setting supports the storage of approximately 103 hours of video.
- The 720p resolution setting captures video at a rate of 1.87 GB per 60 minutes of video. This setting supports the storage of approximately 54 hours of video.
- The 1080p resolution setting captures video at a rate of 4.57 GB per 60 minutes of video. This setting supports the storage of approximately 22 hours of video.
- The 1440p resolution setting captures video at a rate of 9.08 GB per 60 minutes of video. This supports the storage of approximately 11 hours of video.

3. Pre-event audio/video buffer that is configurable by the City.

Yes. Both camera models include a configurable pre-event audio/video buffer. Depending on agency settings, the pre-event buffer can capture up to two minutes (120 seconds) of video immediately preceding event recording and is configurable in 30-second increments. By default, the pre-event buffer is 30 seconds.

Audio recording can be disabled during buffered video recording to accommodate agency evidence collection policies. Audio recording is disabled for pre-event buffering by default.

4. BWC must be able to effectively record in low-light conditions.

Yes. Typically, there is a trade-off between better low-light performance and limiting the blurriness or jumpiness of a video, but with our clear frame technology, the Axon Body 3 and Axon Body 4 balance both.

AXON BODY 3

The Axon Body 3 records in full color and utilizes advanced low-light technology and has a lux rating of < 0.1 lux to mimic the human eye in low light environments. This is important because a lux rating indicates low-light perception capability, which is the level of light required to see an object. Emulating this level of low-light perception when a video is captured allows agencies to leverage evidence that closely represents what an officer saw in the moment.

With an algorithm designed to minimize blurring in fast-moving, low-light environments, the Axon Body 3 is capable of capturing high-quality videos in a variety of circumstances.

AXON BODY 4

The Axon Body 4 utilizes advanced low-light technology and has a lux rating of < 0.1 lux to mimic the human eye in low-light environments. This is important because a lux rating indicates low-light perception capability, which is the level of light required to see an object. Emulating this level of low-light perception when a video is captured allows agencies to leverage evidence that closely represents what an officer saw in the moment.

Our clear frame technology uses an auto-exposure algorithm to analyze both image brightness and scene motion.

For example, if the camera is recording in low-light conditions and there is not much movement in the frame, the camera will use a longer exposure time to minimize noise. Now, in the same lighting conditions, but with more motion, the camera would shorten the exposure time to balance both motion blur and noise.

The algorithm then automatically balances detected noise, brightness, and motion blur to capture clear high-quality video without altering what the camera operator saw. Because of these design choices, the Axon Body 4 can effectively minimize blurring to fast-moving objects, in a variety of low-light environments.

5. The image field of view must be at least 65 degrees vertical, 120 degrees horizontal and 140 degrees diagonal.

Yes. The Axon Body 3 has a 146.4° diagonal field of view, 125.2° horizontal field of view, and 68.6° vertical field of view.

The Axon Body 4 camera has a 140° horizontal field of view, a 76° vertical field of view, and a diagonal field of view of 160° for its default 16:9 aspect ratio setting.

6. BWC must be encrypted.

Yes. While on the Axon Body 3 camera, evidentiary video is protected from manipulation with AES 128 XTS full disk encryption. During transfer, communication between the Axon Body 3 camera and Axon Evidence is conducted over 256-bit AES encryption to safeguard data.

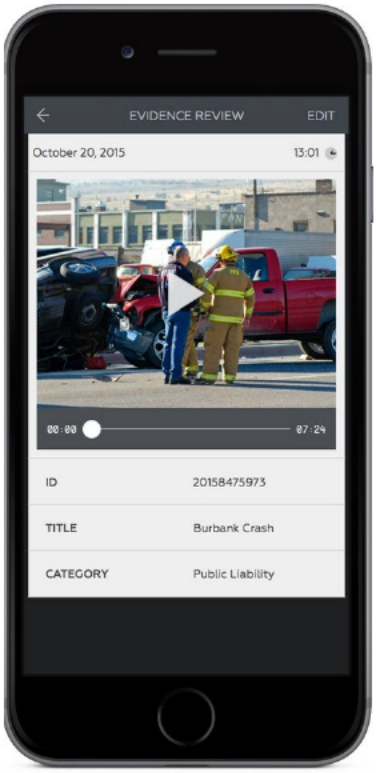
The Axon Body 4 camera protects device data via AES-256-XTS encryption using per-device, unique keys stored in the Qualcomm Secure Execution Environment on the Qualcomm SOC (System-on-Chip).

7. BWC should have immediate playback capability via a separate viewer/smart device/cell phone application.

Yes. Axon View is a free mobile application designed so that users can easily review and tag body-worn camera footage from the field from Axon Body 3 and Axon Body 4 cameras. Axon View can be installed on an Android or iOS device; an authorized user will then log in with their Axon Evidence credentials. The body-worn camera can then be paired with the device by using built-in Bluetooth and Wi-Fi connections.

Once connected, users can view a live feed from the camera, re view videos, or tag recorded videos with the following metadata:

- **ID** – The case ID is agency-dependent and may be generated from a call for service; alternatively, if auto-tagging is implemented, this field can be left blank and the ID will auto-populate after upload.
- **TITLE** – The video title can be updated by the user to display a specific title; by default, the title will contain the device type, date, and time of the video, e.g., Axon Body 3 Video 2022-10-13 1447.
- **CATEGORY** – Custom retention categories from San Diego PD's Axon Evidence account are displayed in Axon View; users can add multiple categories to a given piece of evidence if necessary.



When recorded footage is offloaded from the body-worn camera, the videos will include the tagged metadata without any additional interaction required from the user. Note that Axon View was designed to not store evidentiary data on the smart device for security purposes. Footage cannot be deleted, altered, or edited using Axon View.

6. DESIGN REQUIREMENTS

1. BWC shall be ruggedized and constructed of a highly durable material.

Yes. Both cameras are extremely rugged, securely sealed, and water and shock resistant. The device is a self-contained unit with no fragile moving parts on the exterior. The cameras are designed for durability and undergoes rigorous testing so users can rely on longer-lasting cameras with fewer failures and a lower overall total cost of ownership.

The cameras are impact certified from a height of 6 feet when in normal temperature ranges (ambient). The cameras are also impact certified from 4 feet when in extremely cold temperatures (-4°F and below). Both cameras are tested to and pass MIL-STD-810G Test Methods for vibration, salt fog, and blowing dust resistance. The devices operate normally in up to 95% humidity (non-condensing).

By passing MIL-STD-810G, the cameras adhere to established military standards, which validate product credibility, market competitiveness, and compatibility within the defense and public safety industries.

The most common damage to body-worn camera devices results from a drop; Axon body-worn cameras' ruggedized high-impact polymer protects against damage from this common occurrence, reducing repair and replacement costs as well as downtime. Furthermore, Axon's numerous mounting options are strong enough to hold the camera in place during strenuous activities such as running or fighting.

AXON BODY 3

The Axon Body 3 has an IEC 60529 IP67 ingress protection (IP) rating. This IP rating means the device is dust-tight and highly resistant to water ingress when submerged at a depth of up to 1 meter for 30 minutes. Sensitive internal components are dependably protected against solid and liquid intrusions. Additionally, the camera has an IPX4 rating, which categorizes the device as being resistant to splashing water from any direction.

AXON BODY 4

The Axon Body 4 ingress protection (IP) rating is IEC 60529 IP68, meaning the device is dust-tight and highly resistant to water ingress when submerged at a depth of up to two meters for 30 minutes, thus protecting sensitive internal components from solid and liquid intrusions. The camera also has an IPX4 rating, which categorizes the device as resistant to splashing water from any direction.

2. The City's BWC color preference is black.

Yes. All Axon cameras are constructed of black ruggedized high-impact polymer.

3. The BWC will be no more than 4" in height.

Yes. The Axon Body 3 camera measures 3.8" in height. The Axon Body 4 camera measures 3.95" in height.

4. The BWC will be no more than 3" wide.

Yes. The Axon Body 3 camera measures 2.6" wide. The Axon Body 4 camera measures 2.65" wide.

5. The BWC will be no more than 1.5" in depth.

Yes. The Axon Body 3 camera measures 1.19" in depth (1.03" (D1) X 1.19" (D2)). The Axon Body 4 camera measures 1.21" in depth (1.05" (D1) x 1.21" (D2)).

6. The BWC will be of a weight that does not impede the officer from engaging in normal police activities.

Yes. The total weight of each camera, inclusive of all integrated fastenings for the standard RapidLock mount are:

- Axon Body 3 is 6.9 oz.
- Axon Body 4 is 7.76 oz.

7. The BWC will have an indicator light to show operational status of the camera.

Yes. Both cameras provide visual (LEDs), audible (beeps), and haptic (vibration) feedback to clearly indicate the current mode of operation and alert the wearer of the camera's status.



The camera display screen on top of the camera is divided into a Status Bar and Activity Area. The Operation LED, located on the top of the camera, displays the device's current operating mode to the wearer.

Activity Area Icon	Description
READY	Ready (Buffering) mode
	Recording

The Operation LED, located on the top of the camera, displays the device's current operating mode to the wearer.

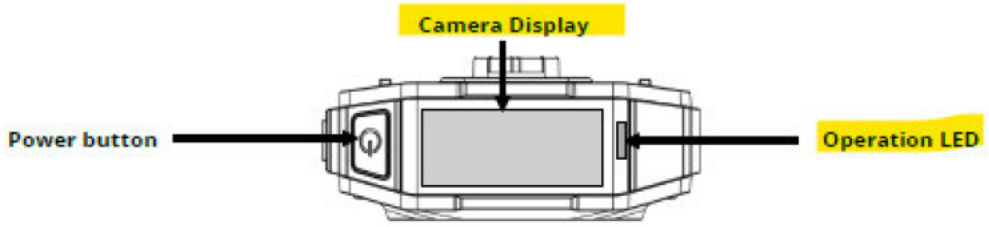
OPERATING MODE	OPERATION LED
Recording	Blinking red
Ready (Buffering)	Blinking green

The triad LED, located on the front of the device also conveys information to the wearer.

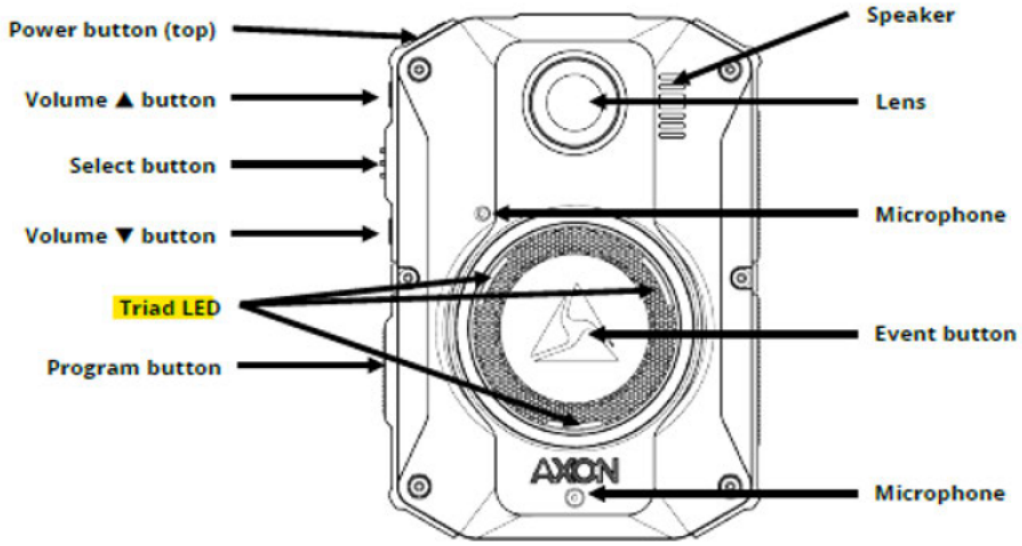
OPERATING MODE	TRIAD LED
Recording	Blinking red
Ready (Buffering)	Blinking green

AXON BODY 3

The following images show the different components on the Axon Body 3 camera.



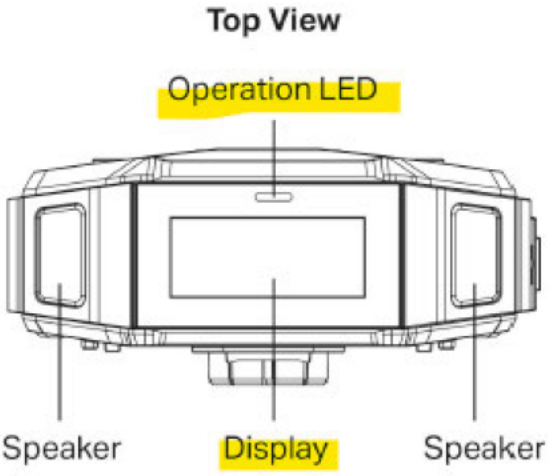
Axon Body 3 Camera top

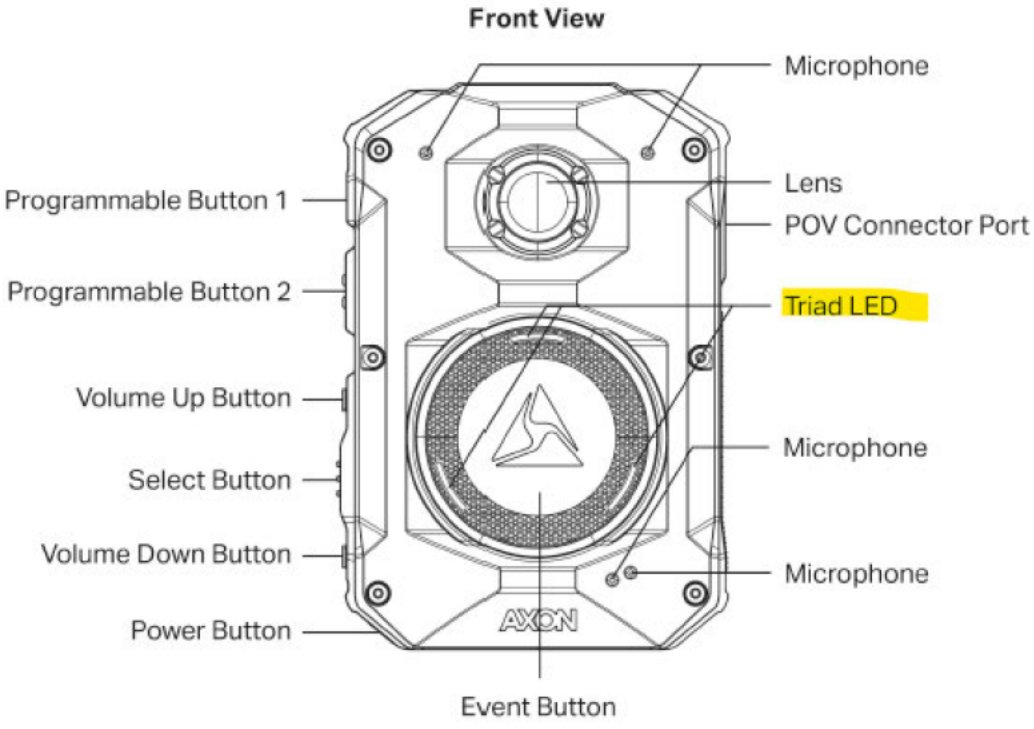


Axon Body 3 Camera front

AXON BODY 4

The following images show the different components on the Axon Body 4 camera.





8. **The BWC will have a display screen which will minimally indicate the battery status and recording status of the camera.**

Yes. The Operation LED, located on the top of the Axon Body 3 and Axon Body 4 camera, displays the device's current recording status to the wearer and includes the following information.

OPERATION LED IN THE FIELD	
OPERATING MODE	**OPERATION LED**
Recording	Blinking red
Ready (Buffering)	Blinking green
Low battery or error	Blinking yellow

The Axon Body 3 and Axon Body 4 have a display on top of the camera which is divided into a Status Bar and Activity Area. The status bar shows the current battery percentage.



9. **BWC shall have an audible chime/beep that sounds intermittently to notify the user that they are in recording mode. The user must be able to control the volume level of this notification including turning it off so they are in "stealth mode."**

Yes. For both the Axon Body 3 and the Axon Body 4 cameras, the audible feedback component complements the visual and haptic features, helping users stay informed even when they cannot divert their attention from the task at hand. In high-stress situations or fast-changing environments, officers can determine the camera's operating mode or status via distinct audio sounds coming from the camera's speakers.

AUDIBLE NOTIFICATIONS AND HAPTIC FEEDBACK		
OPERATING MODE	**AUDIO NOTIFICATION**	**HAPTIC NOTIFICATION (VIBRATION)**
Powering On	Two Short Rising-Pitch Tones	One Vibration – Long Duration
Powering Off	Three Short Lowering-Pitch Tones	One Vibration – Long Duration
Start Recording	Two Short Tones	Two Vibrations – Short Duration
End Recording	One Long Tone	One Vibration – Long Duration
Recording Reminder	Two Short Tones Every Two Minutes	Two Vibrations – Short Duration Every Two Minutes

AUDIBLE NOTIFICATIONS AND HAPTIC FEEDBACK		
OPERATING MODE	**AUDIO NOTIFICATION**	**HAPTIC NOTIFICATION (VIBRATION)**
Stop Recording, Return to Ready	One Long Tone	One Vibration – Long Duration
Volume Up or Down	One Short Tone at the New Volume Level	One Vibration – Short Duration
Axon Respond Livestreaming	Three Short Rising-Pitch Tones	One Vibration – Long Duration
Enter or Exit Mute Mode (Microphone Off)	One Short Tone	Two Vibrations – Long Duration
Enter and Remain in Stealth Mode	No Sound	No Vibrations
Exit Stealth Mode	No Sound	One Vibration – Long Duration
Lights Off	No Sound	One Vibration – Long Duration
Event Marker Captured	No Sound	One Vibration – Short Duration
Enter or Exit Sleep Mode	One Short Tone	One Vibration – Short Duration
Low Battery Notifications – 10% And 5% Battery Capacity	Four Quick High-Pitch Tones	Four Vibrations – Short Duration
Camera Enters Pairing Mode	One Rising Pitch, Followed By One Falling Pitch, Followed by Two Consecutive Rising Pitches	One Vibration – Short Duration

STEALTH MODE

Stealth mode is an Axon Body 3 and Axon Body 4 feature that allows users to turn off all of the camera's lights, sounds, and vibrations. This can be an extremely useful feature when users want to operate the camera but do not want it to be discernable in covert situations.

7. DOCKING STATION SPECIFICATIONS.

The proposer must meet the following docking station specifications:

1. **Availability of multiple docking options including multiple bay and single bay docks.**

Yes. Axon Body 3 and Axon Body 4 cameras are both compatible with two types of docks—an 8-Bay Dock and a 1-Bay Dock.

2. **Primary video upload method must be via a docking station which allows BWC to upload videos and charge its battery at the same time.**

Yes. While the primary purpose of the Axon Docks is camera charging, they serve additional functions by providing a secure connection to our DEMS, Axon Evidence. This connection enables the secure uploading of evidence, receiving the latest operating system updates, and facilitating agency-wide setting changes. Furthermore, the docks serve as a means to register an agency's entire set of cameras.

Plugging a camera into the dock automatically initiates all of these processes, requiring little to no user interaction after the camera is docked. It is worth noting that cameras do not need to be assigned to specific docks, as the docks work as universal charging solutions, Ethernet adapters, and unmanaged network switches. As a result, Axon Body 3 cameras are compatible with any Axon Body 3 Dock, and Axon Body 4 cameras are compatible with any Axon Body 4 Dock. This means that regardless of the specific dock chosen, the camera will begin charging and establish a network connection upon insertion. The docks are equipped with all essential cables required for operation, including a compatible external power supply and Ethernet cable. They can be easily connected to an available power outlet and positioned according to an agency's preference and based on available space.

Overall, the Axon Dock offers a seamless and efficient solution for charging, data management, and network connectivity for Axon cameras. The multiple dock options provide agencies with the flexibility they need to effectively support their body-worn camera deployment.

3. **Attachment to a computer cannot be the primary method of uploading videos.**

Yes. The primary method of uploading is via a dock. Both the Axon Body 3 and the Axon Body 4 use an eMMC to store data, which is populated directly on the circuit board rather than using an SD card, thus requiring the destruction or modification of the circuit board to access data. Additionally, videos cannot be deleted from the camera, and cameras will not natively mount into a Microsoft Windows operating system like a mass storage device such as a flash drive or external hard drive would.

8. VIDEO MANAGEMENT/ STORAGE SYSTEM SPECIFICATIONS

The proposer must meet the following video management system specifications:

1. Unlimited video storage.

Yes. Axon's proposal includes unlimited storage from Axon generated devices – body-worn cameras, Axon Capture, and Axon Citizen. Axon Evidence is by nature, highly scalable; your agency may acquire storage as needed without limit, in accordance with storage purchased.

2. User-friendly video management system.

Yes. Axon Evidence's simple but feature-rich layout presents an intuitive flow of digestible information for its users. With easy-to-use navigational tabs, a dynamic interface, and bulk action capabilities, users can manage, search, and access evidence with speed and efficiency. We have provided detailed information regarding the management functions of Axon Evidence below, including navigation, user interface, bulk actions, camera setting configuration, and video evidence management/viewing.

EASY-TO-USE NAVIGATIONAL TABS

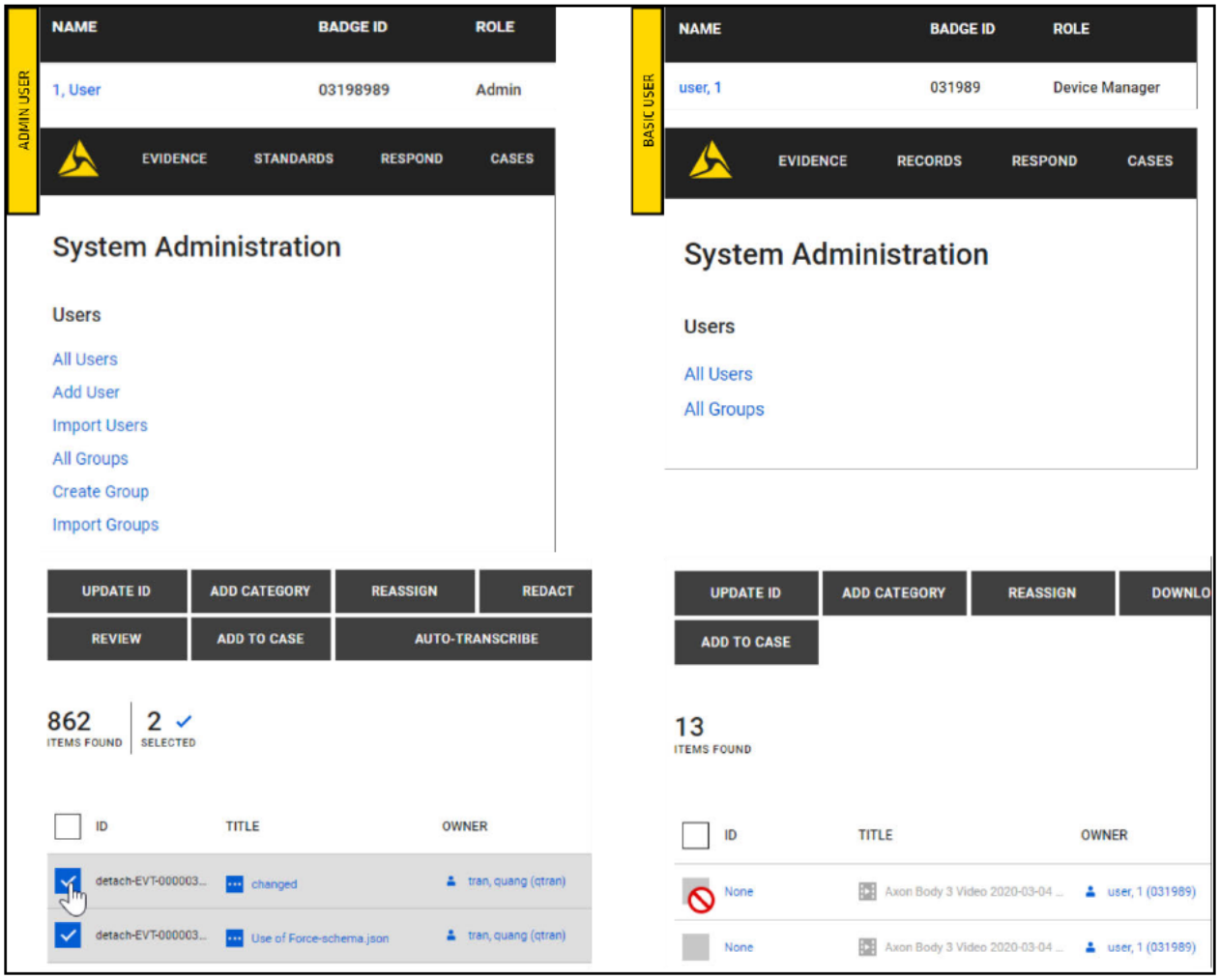
When using Axon Evidence, users will interact with the navigational tabs at the top of the webpage to navigate the system. These tabs are as follows:

- **DASHBOARD** – Provides a high-level view of a user's account and system usage
- **EVIDENCE** – Allows users to search and view evidence
- **RESPOND** – Allows users to access real-time awareness functionalities
- **CASES** – Allows users to build, search, share, and manage cases
- **INVENTORY** – Allows users to manage devices, information, and returns
- **REPORTS** – Allows users to create and download system reports
- **ADMIN** – Allows administrative functionality to control agency settings, *e.g.*, security, roles and permissions, categories, retention, etc.
- **HELP** – Allows users to access release notes, the help center, Contact Us support, and necessary software

DYNAMIC USER INTERFACE

Axon Evidence implements a dynamic user interface that adjusts to a user's permissions within the system. For example, an Admin user will most likely have access to more tools and actions than that of a Basic user. Depending on those permissions, a user's experience in the system will vary. By providing a specific user with only the actions necessary to complete their duties when working within Axon Evidence creates a cleaner workspace with fewer distractions. No more mouse clicks that trigger unwanted actions or navigating through hundreds of unnecessary evidence files.

The sample screenshot provided compares how different the system can look depending on a defined role. As you can see, the sample Admin user has access to more settings and can bulk edit and view evidence files, while the Basic user only has access to a couple of settings and can view evidence by metadata.



BULK ACTION

Axon Evidence also supports bulk action capabilities that can save a user time when managing the system and their evidence. For example, instead of going into the video player interface to perform actions on an individual video, Axon Evidence supports bulk actions that can be performed on one or many selected videos based on search results, which can save time when managing multiple pieces of evidence. These actions include Update ID, Add Category, Reassign, Redact, Download, Share, Delete, Restore, and Export.

CONFIGURING CAMERA SETTINGS

All body-worn camera settings are managed within “Body Camera Settings” in the Admin tab. This includes adjusting camera settings and activation indicators such as the front ring light.

- Video quality
- Pre-event buffer (both the duration as well as audio on/off)
- User-configurable Stealth mode and indicator lights
- Front ring LED
- Watermark
- Bookmark
- Audio on / off
- Auto-activation triggers are managed within “Signal Configuration,” also found in the Admin Tab. Signal Configuration allows the administrator to manage the different triggers.

SEARCHING FOR EVIDENCE

While searching, a user can immediately specify whether they want to search “All Evidence” or “My Evidence”. This is very useful because usually, an officer is dealing with their own evidence.

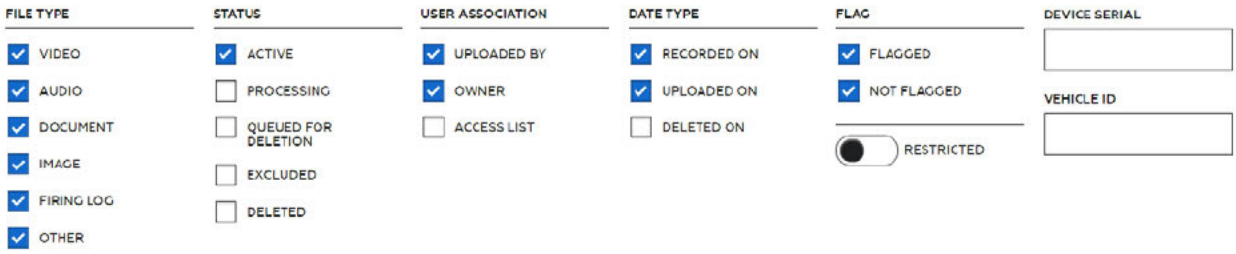
Axon Evidence provides both “Basic” and “Advanced” search capabilities. This is similar to how Google or other search engines provide the ability to search by common criteria (basic), or if required, more detailed (advanced) search criteria. Basic searches include:

- ID (Incident Number)
- Title
- User or Group (Person who recorded the video)
- Date and Time
- Category (Incident Type)
- Tags



If a user requires more granularity in their search, they can click “Show Advanced Search” and they will have the additional search criteria:

- File Type (Video, Audio, Document, Image, Etc.)
- Status (Active, Processing, Queued for Deletion, Deleted, etc.)
- User Association (Uploaded By, Owner, Access List)
- Date Type (Recorded On, Uploaded On, Deleted On)
- Flag (On/Off)
- Restricted Access (On/Off)
- Custom Metadata



ADDITIONAL SEARCH FUNCTIONALITY

- **AUTO-COMPLETE** – Certain fields will adapt and shorten the drop-down list as the user inputs more information (e.g., Name, Group, etc.). For long lists such as "User", this greatly speeds up the process of searching. An officer only has to type in the first few letters and the application will adapt the drop-down list.
- **AUTO-UPDATE** – Search results will auto-update. For example, if an officer only has incomplete information about a video, they can rapidly search different variations without the need to repeatedly hit enter or click “search”. The search results will automatically update based on the given inputs.

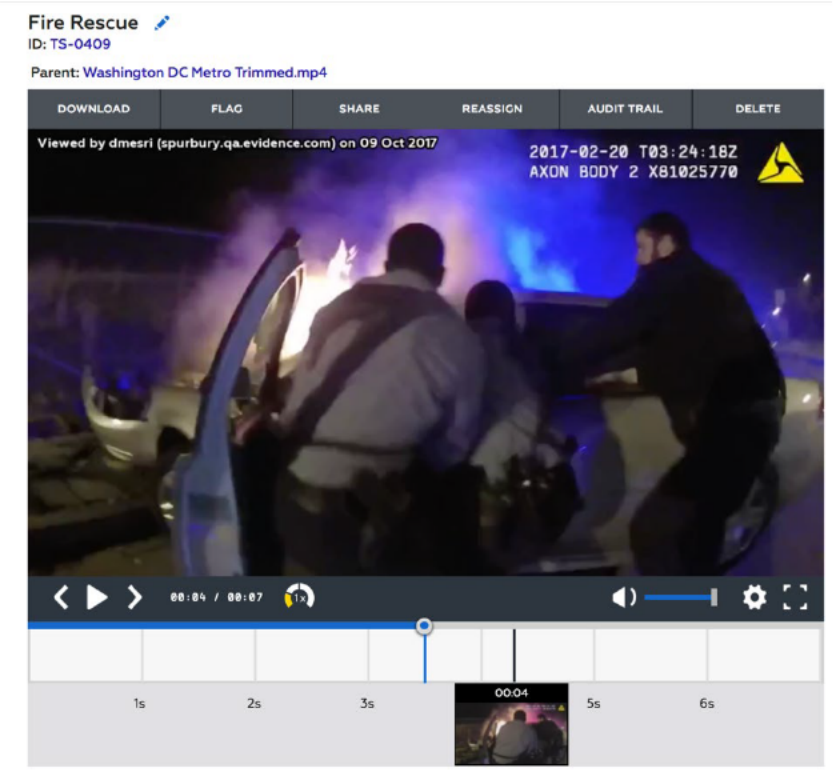
SEARCH RESULTS

Search results can be displayed in the Gallery or Table format. Gallery gives a thumbnail making it easy to identify videos with similar metadata, Table format is useful for comparing metadata. Results can also be sorted by ID, Title, Upload Time, as well as Record Time.

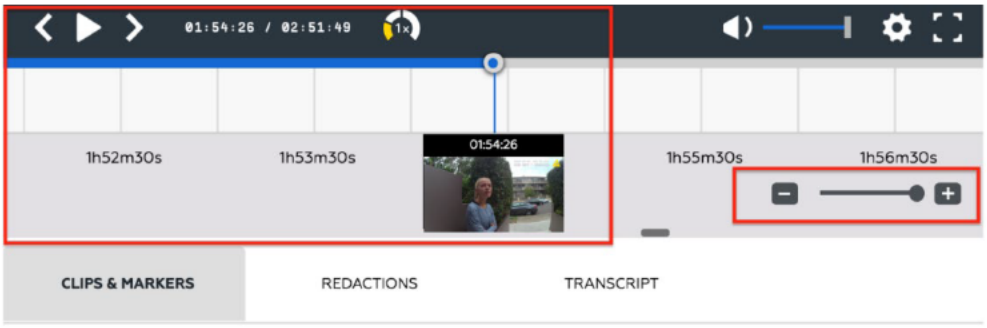
VIEWING EVIDENCE

Axon Evidence’s media player is designed to be very intuitive, similar in many ways to the well-known YouTube player. The tools presented will adjust automatically depending on the type of evidence being viewed. For example, a slightly different toolset is shown when viewing a still image than a video.

For videos, the player incorporates tools for a simple review of evidence. The player has the capability for frame-by-frame playback (forwards and backward) as well as auto-generated thumbnails in the button scrubber bar.



The player interface also provides a "zoom slider" on the right. This allows SDPD to adjust the increments displayed on the scrubber. Zoom out and you can see the entire video (start to finish); zoom in and focus in on specific seconds. This makes it easier for SDPD to rapidly scroll to the approximate time and then "zoom in" to place markers precisely.



Playback also supports up 1x, 2x, and 4x playback speed. Based on customer feedback, it was identified that one of the biggest inefficiencies deals with reviewing longer videos. Additionally, for in-car videos (Axon Fleet) with embedded speed metadata, the speed can be overlaid in the bottom right of the video.



3. **Ability to export video in an industry standard file format.**

Yes. Video and audio are recorded and exported in MP4, an industry standard, standard, open, and non-proprietary format (including both codec and container).

Audio and video are recorded as the same MP4 encoded file, ensuring perfect synchronization. The video format is MPEG4, using the H.264 compression standard. Sound is recorded via the Advanced Audio Coding (AAC), a coding standard for lossy digital audio compression. The MP4 files can be played using all freely available standard software (e.g., Windows Media player, Real Player, QuickTime, VLC).

4. **Acknowledgment that all data is property of the City and must be made available at no additional cost.**

Yes. All digital evidence stored on Axon Evidence is owned by SDPD. Axon's contracts are constructed to ensure that our customers retain all ownership of their data.

5. **Storage solution compliance with policies outlined in the U.S. Department of Justice Information Services (CJIS) Security Policy and the City of San Diego Information Security Standards and Guidelines. See attached links for further information. CJIS Security Policy 2022 v5.9.1 — FBI. Microsoft Word - AR 90- 63 Information Security FINAL 2011-06-28.docx (sandiego.gov).**

Yes. Axon Evidence was designed and is operated to ensure that it is compliant with the FBI CJIS Security Policy. Customers can be assured that their digital data is protected by a robust information security program that is designed to exceed the CJIS security requirements as well as provide protection against current and emerging threats.

Axon acknowledges and abides by all aspects of the CJIS Security Addendum, and we are contractually committed to meeting CJIS, as the CJIS Security Addendum is included by reference into the Axon Master Services and Purchasing Agreement.

All Axon CJIS-authorized personnel are required to complete CJIS security training in compliance with the CJIS Security Policy. Axon uses 'CJIS Online' from Peak Performance Solutions to conduct and coordinate CJIS-specific security training. Axon personnel training records are available to customers within the CJIS Online System. Any additional SDPD-specific security awareness training can be conducted as required.

In addition to security awareness training, Axon CJIS-authorized personnel have undergone state and federal fingerprint-based checks in certain states. Axon is prepared to coordinate with SDPD to ensure that all Axon CJIS-authorized personnel undergo checks in alignment with the requirements of SDPD.

Axon's CJIS compliance status has been validated independently by CJIS ACE and the underlying security program is audited on at least an annual basis by an additional third party as part of Axon's ISO 27001 program.

The Axon CJIS Compliance White paper (found here) outlines the specific security policies and practices for Axon Evidence and how they are compliant with the CJIS Security Policy. We have also provided information regarding our security compliance certifications below, as additional detail regarding this topic.

6. Capability to produce digitally authenticated duplicates.

Yes. Evidence integrity is a primary function within the Axon platform; the application provides customers with comprehensive access control features, enabling you to customize access to your evidence data. Every evidence file within Axon Evidence is complemented by a detailed, tamper-proof audit trail, which is maintained to provide chain of custody reporting. This audit trail includes evidence metadata along with a detailed record of the "who, when, and what" for every interaction with the piece of evidence.

During transfer, a SHA-2 checksum is generated for each video. Once a video lives in Axon Evidence, it can be duplicated as desired. These duplicates are known as child assets. Unmodified child assets will pass the SHA-2 checksum throughout the lifetime of the asset. The SHA-2 cryptographic hash function is applied to each MP4 video, and functions as a digital fingerprint for each video captured. These checksums are then compared as part of the upload process to Axon Evidence to confirm that a file has not been compromised during the upload process. If a checksum mismatch occurs, the upload process is reinitiated.

Within the Axon Evidence application, the SHA-2 checksum is viewable by users with access to the evidence audit trail for the specific piece of evidence. These tamper-proof audit trails are created automatically by Axon Evidence upon ingestion of any evidence file. Audit trails are stored in a highly secure database and can be viewed, in a read-only format, by agency users with the appropriate permissions within Axon Evidence. Audit trails include all activity and interactions with the evidence file, and each log record is accompanied by a timestamp. Audit trails cannot be edited or changed, even by agency administrators.

7. Cloud-based storage.

Yes. Axon Evidence is a cloud-hosted digital evidence management solution provided as a service (SaaS) application. It is horizontally scalable and can elastically adapt to accommodate any traffic volumes. Internally, the solution uses a service-oriented architecture where functionality is provided by discrete compassable services that can run on one or many servers. This allows individual components to scale to handle changes in traffic volumes.

The application supports uploads from multiple users, devices, and locations, simultaneously from thousands of agencies across the continental United States.

8. Ability for retrieve/search video footage.

Yes. The search functionality in Axon Evidence is designed to minimize the time spent by a user trying to locate a video file. The search interface consists of a simple layout, while still providing advanced searching capabilities and additional controls for how search results are displayed. Search results are automatically updated as users enter filter information.

To filter search results, a user enters specific information or metadata—such as an evidence ID, owner, or date. Those entries will help reduce an agency's entire catalog of evidence down to a condensed list of relevant evidence. In addition to standard metadata filters, the Evidence Search page supports filtering evidence by agency-specific custom metadata fields within the advanced search section to narrow the results further, as described below.

EVIDENCE SEARCH FILTERS

A user can start a search from any of the following search pages:

- **ALL EVIDENCE** – Populates all evidence in an agency's instance of Axon Evidence, regardless of ownership or permissions
- **MY EVIDENCE** – Populates only the evidence associated with the user
- **SHARED EVIDENCE** – Populates evidence that has been shared
- **EVIDENCE MAP** – Populates evidence with location data attached
- **CITIZEN EVIDENCE** – Populates evidence that has been submitted via a Citizen public portal or invite



STANDARD EVIDENCE SEARCH FIELDS



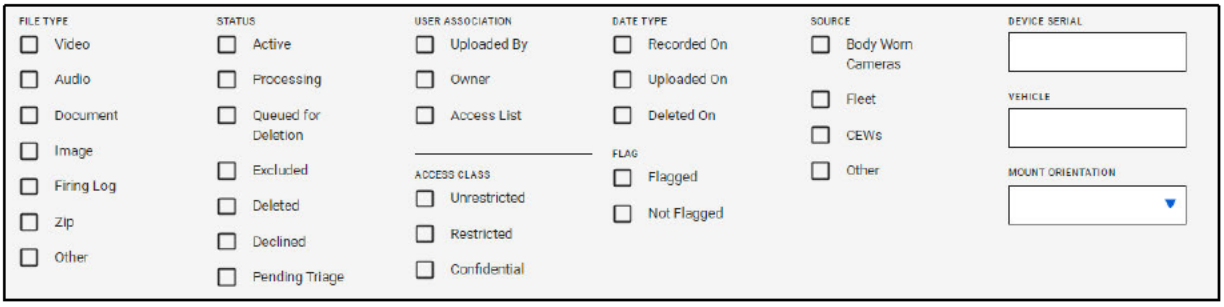
- **ID** – Limits search results to evidence with an ID that includes the characters entered in the ID field; to search for evidence without an associated ID, a user can enter "None" in the ID field
- **TITLE** – Limits search results to evidence with a title that includes the characters entered into the Title field
- **USER OR GROUP** – Limits search results to evidence owned by a user or members of a group specified; if searching from the My Evidence page, their user name will automatically populate in the User or Group field
- **DATE** – Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected; users must specify dates by using the From and To boxes to populate inclusive evidence captured within the specified date range
  - **FROM** – The start of the date range. If the From box is empty, the date range begins with the earliest date

- **TO** – The end of the date range. If the To box is empty, the date range ends with today.
- **TIME** – Users can select the time in hour and minute increments via the Start and End parameters in the Date search filter (From and To)
- **NOW** – Users can click the Now button within the Date search filter (From and To) to quickly search for evidence submitted to the system on the same day

- **CATEGORY** – Limits search results to evidence assigned to the category selected; by default, search results include evidence assigned to any category, including uncategorized evidence; to search for evidence without an associated category, a user can enter "None" in the ID field
- **TAG** – Limits search results to evidence with tags that include the characters you enter in the Tag field; To search for evidence without an associated category, a user can enter "None" in the Tag field
- **CUSTOM METADATA** – Limits search results to show evidence associated with custom metadata created by an agency
- **CASE ID** – Search results will display pieces of evidence that are grouped in cases with the specified case ID name or number.

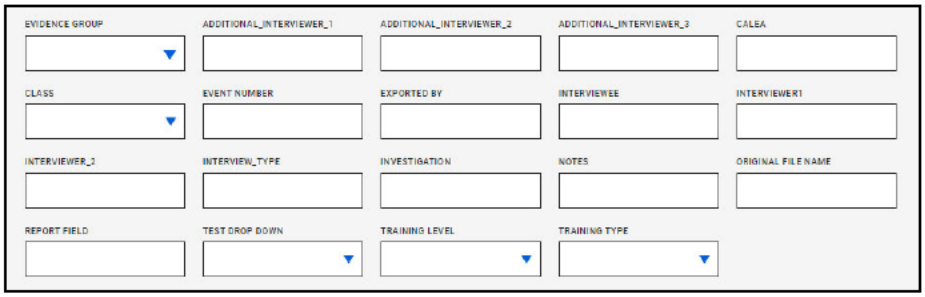
ADVANCED EVIDENCE SEARCH FIELDS

If a user requires more granularity in their search, they can click the Show Advanced Search button, which will display additional search criteria options.



- **FILE TYPE** – Limits search results to the selected file type; by default, search results include all file types
- **STATUS** – Limits search results to evidence with a specific status; by default, an evidence search will populate Active evidence
- **USER ASSOCIATION** – Limits search results to evidence uploaded or owned by a specific user, as well as what access lists their evidence is associated with
- **DATE TYPE** – Limits search results based on when a piece of evidence was recorded, uploaded, or deleted
- **FLAG** – Limits search results to evidence with either a Flagged or Unflagged status

- **SOURCE** – Limits search results to evidence from the selected device type that produced the evidence file; the categories include Body Worn Cameras, Fleet, CEWs, and Other (which includes evidence with no device type and evidence that has been extracted and redacted)
- **DEVICE SERIAL NUMBER** – Limits search results to evidence from a particular device, which can be useful when making bulk edits
- **VEHICLE** – Limits search results to evidence from a particular vehicle
  - This field only appears if an agency uses Axon Fleet, and the vehicle has been added to an account with the Vehicle configuration
- **MOUNT ORIENTATION** – Limits search results to evidence captured by a specific in-car camera (Front or Rear)
  - This field only appears if an agency uses Axon Fleet, and the vehicle has been added to an account with the Vehicle configuration
- **CUSTOM METADATA** – Allows users to search for evidence by custom metadata fields created by your agency and users; custom metadata fields will appear as empty entry fields labeled by custom metadata type



ADDITIONAL SEARCH FUNCTIONALITY

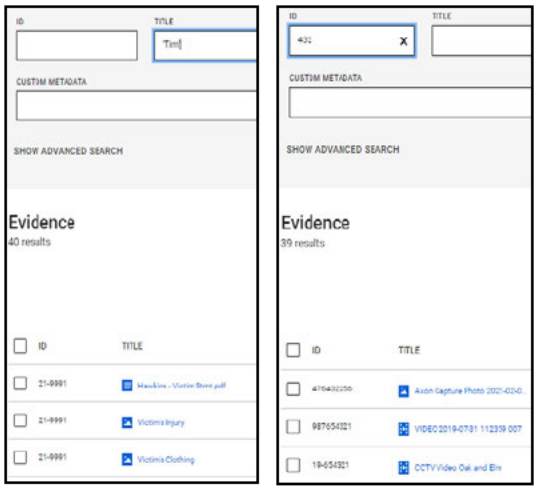
- **AUTO-COMPLETE** – If a user places their cursor into a certain text field or types in characters, the field will generate a short drop-down of search recommendations
- **AUTO-UPDATE** – As a user types characters into a search field, checks a box, or selects an item from a drop-down list, the search results will update in real-time
- **MULTIPLE PARAMETERS** – As part of our basic and advanced search functions, a user can search by any desired combination of the parameters available
- **SPECIFIC PARAMETER** EXCLUSIONS – As part of our basic and advanced search functions, a user can search by excluding any desired combination of the parameters available
- **DEFINED PARAMETERS USING "WILDCARD" SEARCH** – As part of our basic and advanced search functions, a user can specify certain parameters, and then add information to any free-form text field to search with more granularity
- **SPECIFIED RANGES** – Axon Evidence supports a variety of searches based on a specified range of either time or date

Please note that all search results are based on user access, so, if a user does not have access to certain evidence, that evidence will not be accessible from the search results.

SEARCH LANGUAGE OR SYNTAX

Axon Evidence search functions do treat all values and strings in a free-form text field as OR and wildcards instances.

For example, if a user types in **"Tim"** in the **Title** field, the search results may include pieces of evidence with words like **victim** in the title. Furthermore, if a user were to type **432** in the **ID** field, the search results may yield pieces of evidence with an ID that includes the number 432, such as 476432256.

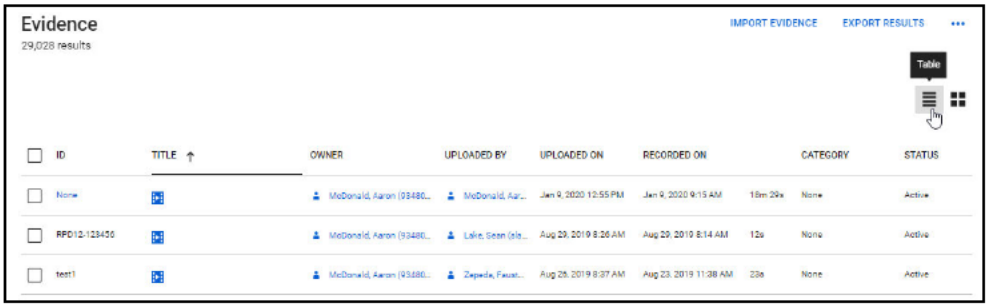


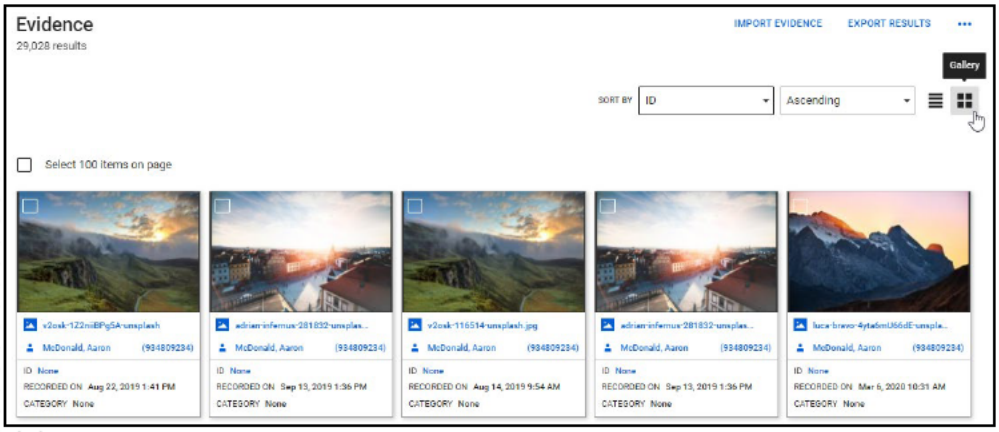
SEARCH RESULTS

When search results are populated, only evidence files that match the established search criteria of a user will be shown. When a search is complete, users can then select how they view and sort the evidence.

VIEWING SEARCH RESULTS

Search results can be shown in a table view (default) or a gallery view.





SORTING AND FILTERING SEARCH RESULTS

By default, search results are displayed in the order of the most recent **Recorded On** times; however, users can also filter search results by the following filter columns: **ID**, **Title**, **Uploaded On**, and **Recorded On**. By simply clicking on the desired filter column display name, the evidence list will repopulate to meet the selected filter criteria.



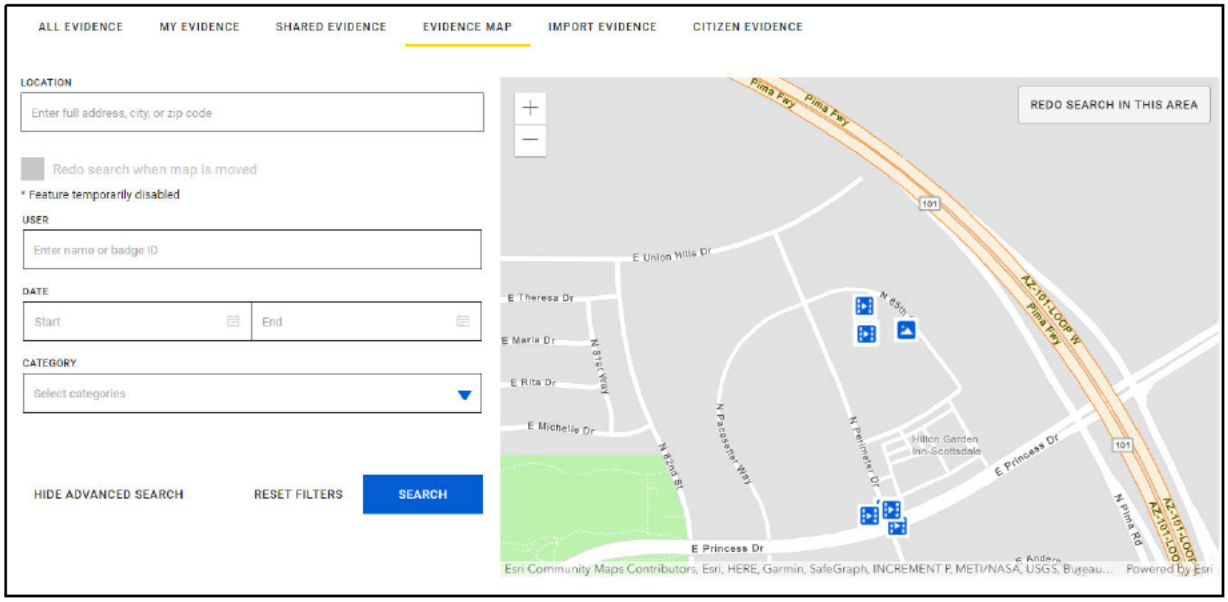
USING THE EVIDENCE MAP PAGE

When searching for evidence on the **Evidence Map** page, users can view evidence displayed either on the map—as a file-type icon—or via the **Table** and **Gallery** views. The map icon used for an evidence file is determined by the evidence type and corresponds with the six icons shown here.



To view the evidence in different areas on the map, a user can use their computer mouse to adjust the location by clicking and dragging within the map window. A user can also zoom in and out by clicking the + and – icons located in the top left-hand corner of the map, or by using the wheel on your mouse.

Search functionality on the Evidence Map page allows users to search for evidence by **Location**—which includes the address, city, or zip code—as well as **User**, **Date**, and **Category**.



9. Comprehensive metadata storage capability.

Yes. Numerous metadata tags can be applied to evidentiary assets. These metadata fields are included in the searching interface to help you locate the evidence you need quickly and efficiently. ID, title, notes, and tags are free text, user-defined values. Custom metadata fields will also be available to narrow search results on the advanced search page.

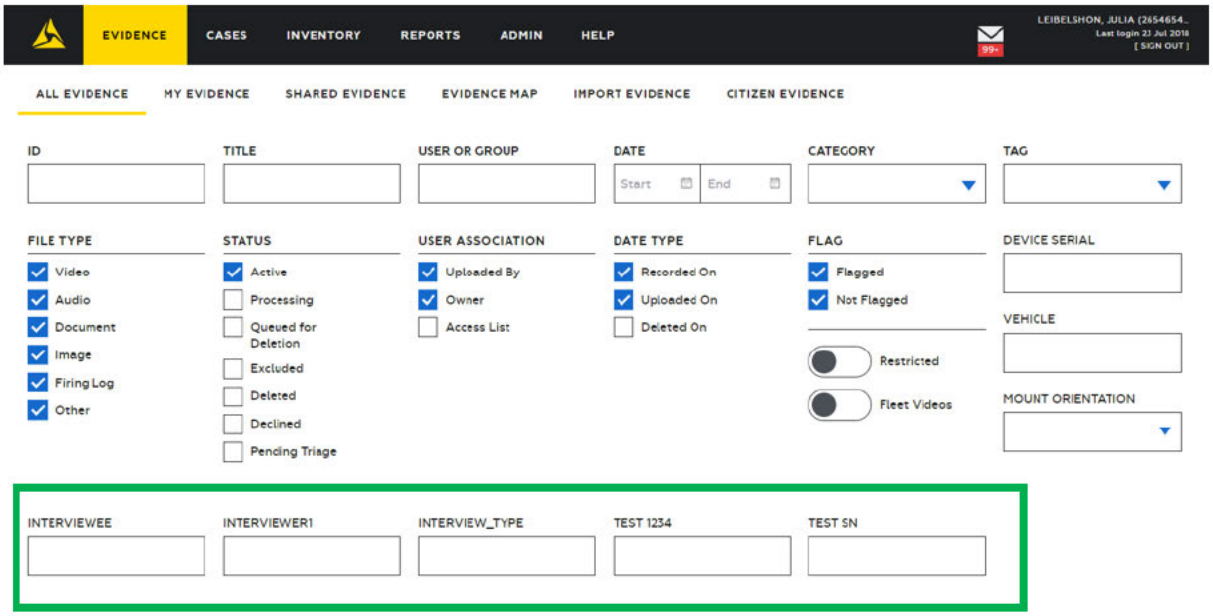


Figure 1 Custom metadata fields will populate in the advanced search field

Once a user locates a file, they can add or update the following metadata. All changes are captured in the evidentiary audit log. Users can add the following standard metadata (in addition to defining custom agency-specific metadata fields).

- **TITLE AND ID** – On the Evidence Detail page, the evidence title and ID appear in the upper-left corner.
  - An evidence title can be up to 256 alphanumeric characters. By default, the title populates with the camera type, date, and time (AXON Fleet 2 Video 2018-07-23 1654).
  - An evidence ID can be up to 75 alphanumeric characters by default. The evidence ID field can be used to associate a file with the correlating CAD/RMS or incident ID.
- **DESCRIPTION** – Descriptions of the evidence can be added or edited.
- **RECORDED ON DATE AND TIME**
- **TAGS** – Tags are labels that you can apply to evidence and cases. On the evidence search page, a dropdown appears in the Tag search field and will display all tags in the system associated with evidence. Once you perform a search, you can then sort the results by ID, Title, etc.
- **LOCATION** – The specified location for evidence determines where the pin representing the evidence appears on evidence maps.

- **NOTES** – Notes can be posted about evidence. In addition to the text of the note, Axon Evidence shows the author of the note and the date and time that the note was created and updated.
- **CATEGORIES** – The evidence category determines the following. An unlimited number of custom categories (and associated retention periods) can be created and applied to your agency's evidence.
  - Whether the system will initiate automatic deletion of evidence assigned to the category.
  - How long the system waits before initiating the deletion of evidence that is not included in a case. Axon video deletions are based on the recording date. Deletion of all other evidence is based on the upload date.
- **EXTEND RETENTION PERIOD** – If evidence is scheduled for deletion, users can extend how long the system retains the evidence before adding it to the deletion queue
- **FLAGS** – You can flag evidence that you want to find more easily in the future. Evidence searches allow you to filter the search results by the flag status of evidence.
- **REASSIGN EVIDENCE** – The user to whom the evidence is assigned becomes the owner of the evidence
- **VIEW EVIDENCE WITH SAME ID** – If multiple files have the same ID as the evidence being viewed, a paginated table of evidence with the same ID shows the title, owner, and upload date of each evidence file

CUSTOM METADATA

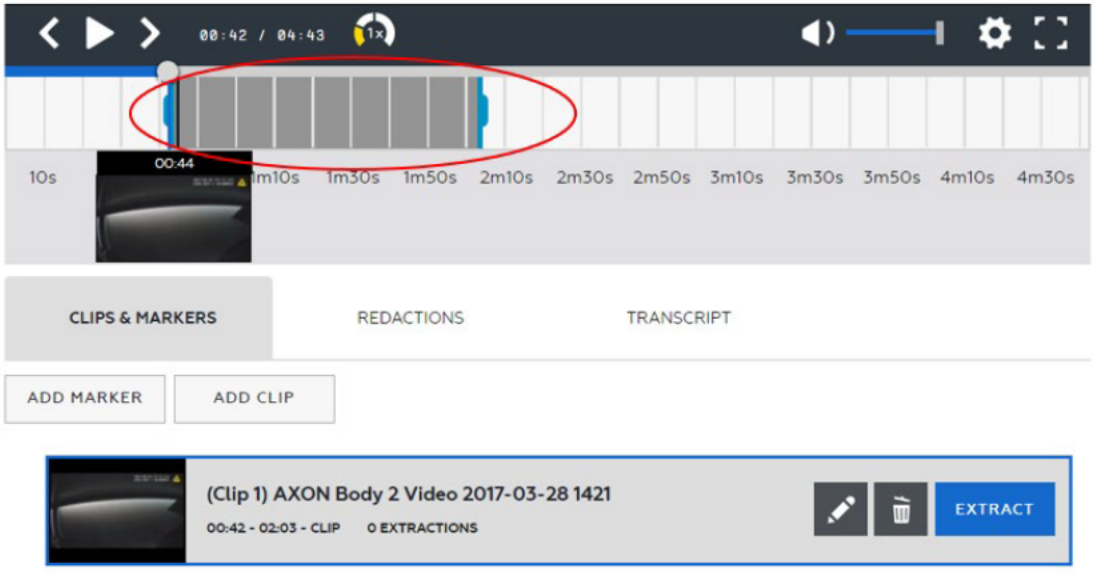
Custom metadata fields will appear below the standard metadata fields next to every evidentiary file. The feature supports three types of custom metadata fields:

- **FREEFORM** – This is a free-form text entry field.
- **VALIDATED** – This is a free-form entry text field, but the entry must conform to the Regular Expression (Regex) definition for the field. This field type can include a description to help users properly enter information.
- **DROP-DOWN** – The user is presented with a list and selects information.

10. Storage system must be able to quickly extract segments of needed footage.

Yes. Users can quickly extract segments of needed footage from storage via the "clipping" functionality built into Axon Evidence. A clip is a continuous segment of an evidence file that can be created to separate an important moment in a video, and easily accessed and played back at a later time when a review is needed. Users with whom you share the evidence can then locate and play clips you have created, as well as view their title and description. This makes sharing only a portion of an evidence file simple, while also identifying that it came from a larger evidence file.

Additionally, having access to shorter evidence files can help reduce the time it takes to complete redaction tasks.



11. Audit trail capability.

Yes. Evidence audit trails are created for every evidence file and list all related actions, as well as associated metadata. All changes made to videos and associated metadata (including, but not limited to, reassigning a video, sharing a video, renaming a video, redactions, and deletions) are logged in the evidence audit trail (including information about the date, time, and user who made the change). You can generate an audit trail for the entire history of the file or view a portion of an audit trail, limiting the report to actions that occurred within a specified timeframe.

The original data associated with a video is never changed; all modifications are handled by creating new, derivative files. To ensure chain of custody, evidentiary files can be verified for authenticity by matching the SHA-2 hash of the original file ingested in Axon Evidence to that of any copy created.

Audit trails are never deleted, even after the video file is deleted. The method of deletion (e.g., system-initiated based on retention policy versus manual deletion by a user with the appropriate permission) will be displayed in the audit trail.

Various actions are shown below as they appear in an audit trail.

SHARING EVIDENCE

15	17 Aug 2017	14:27:43 (-04:00)	**Hassan, Adam (Badge ID: ahassan)** Username: ahassan@taser.com User ID: 5bcf5c0cd7cf4e66afe2684c2c4a6b30	Evidence Record Downloaded; Internal Record ID: FILE:01ADE429A1464A0195A641EE0DF449EE@2827B6323C434D9F92F138143DCE6C6C Client IP Address: 209.115.232.249
16	17 Aug 2017	14:32:16 (-04:00)	**Hassan, Adam (Badge ID: ahassan)** Username: ahassan@taser.com User ID: 5bcf5c0cd7cf4e66afe2684c2c4a6b30	Shared with Barker, Matt (Badge ID: mbarker, Agency: TASER Demo Site) with permissions to View, Download, View Audit Trail, Post Notes and Re-Share. Share expires on 15 Nov 2017 13:32:15 (-05:00)
17	17 Aug 2017	14:32:17 (-04:00)	**Hassan, Adam (Badge ID: ahassan)** Username: ahassan@taser.com User ID: 5bcf5c0cd7cf4e66afe2684c2c4a6b30	Shared with Cooper, Randall (Badge ID: 9897709987, Agency: TASER Prosecutor) with permissions to View, Download, View Audit Trail and Re-Share. Share expires on 15 Nov 2017 13:32:15 (-05:00)
18	17 Aug 2017	14:32:17 (-04:00)	**Hassan, Adam (Badge ID: ahassan)** Username: ahassan@taser.com User ID: 5bcf5c0cd7cf4e66afe2684c2c4a6b30	Shared with Hassan, Adam (Badge ID: 029990ddb90f, Agency: my.evidence.com) with permissions to View. Share expires on 15 Nov 2017 13:32:15 (-05:00)
19	17 Aug 2017	14:32:48 (-04:00)	**Hassan, Adam (Badge ID: ahassan)** Username: ahassan@taser.com User ID: 5bcf5c0cd7cf4e66afe2684c2c4a6b30	Shared with Hassan, Adam (Badge ID: 029990ddb90f, Agency: my.evidence.com) with permissions to View. Share expires on 24 Aug 2017 14:32:15 (-04:00)
20	17 Aug 2017	14:32:58 (-04:00)	**Hassan, Adam (Badge ID: ahassan)** Username: ahassan@taser.com User ID: 5bcf5c0cd7cf4e66afe2684c2c4a6b30	Removed sharing with Barker, Matt (Badge ID: mbarker, Agency: TASER Demo Site)

UPDATING NAME/TITLE

17	18 Aug 2017	11:46:20 (-07:00)	**Smith, Joe (Badge ID: 265465464)** Username: jsmith User ID: 93106c61e5414e34b39ec306f52d9baf	Evidence title updated to 'Test Rename'

REASSIGNING EVIDENCE

13	18 Aug 2017	11:40:11 (-07:00)	**Harris, Tom (Badge ID: 265465464)** Username: tharris User ID: 93106c61e5414e34b39ec306f52d9baf	Reassigned to Smith, John Badge ID: 212365464, Agency: Demo Site)

CREATING A REDACTION

22	11 Aug 2017	11:27:55 (-07:00)	**Kimble, Richard (Badge ID: dougs)** Username: dougs User ID: 8f25be2b2a0d48748450e5c66cfe4ead	Video Clip Edited "(Redaction 1) 05_Redaction_Flex2_02.mp4" (00:00:00 to 00:00:28)

DELETION OF EVIDENCE (AND METHOD OF DELETION)

6	27 Jul 2017	09:03:22 (-07:00)	**Uribe, Bryan (Badge ID: buribe)** Username: buribe User ID: 26183731e1f941229bf44a37c27663a7	Delete Request Received
7	27 Jul 2017	09:03:22 (-07:00)	**Uribe, Bryan (Badge ID: buribe)** Username: buribe User ID: 26183731e1f941229bf44a37c27663a7	Queued for Deletion Comment: demo Deletion is now scheduled for 03 Aug 2017 09:03:22 (-07:00)
8	28 Jul 2017	11:13:25 (-07:00)	**South, Jason (Badge ID: 9900)** Username: jsouth User ID: 3b87519db5814dc39ead8e7e98dd882b	Evidence Record Accessed. Client IP Address: 74.206.119.243
9	03 Aug 2017	09:42:06 (-07:00)	**System**	Deleted

AUDIT TRAILS

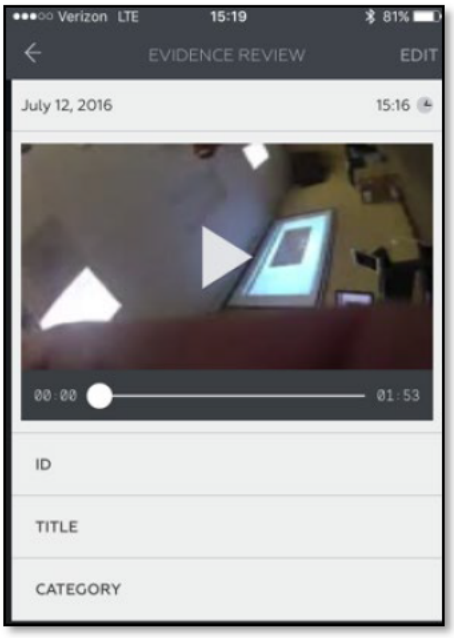
Detailed audit logs track all evidence access and activity. Each audit trail entry shows the date, time, user, and details of each action. You can view the entire audit log or a portion of an audit trail, limiting the report to actions that occurred between a specified timeframe.

- **AGENCY AUDIT TRAIL** – The Agency Audit Trail shows agency-wide changes to your Axon Evidence account. This report helps provide transparency on administrative actions across Axon Evidence. By displaying each action in detail, your agency can review who changed a setting, to understand the purpose and provide better accountability to each user. Only users with the "Edit Agency Settings permission" enabled can view the Agency Audit Trail.
- **USER AUDIT TRAIL** – A User Audit Trail shows many of the activities performed by the user, changes to the user account, and evidence-related user actions. In addition to evidence-related user actions, the User Audit Trail will show failed login attempts, when a user is locked out of their account due to multiple failed login attempts or when a user's password has been reset or their account has been unlocked.
- **CASE AUDIT LOG** – The audit trail entry for Cases shared with a partner agency group use the same audit trail format as Evidence that is shared with a partner agency group. When a Case is shared with a partner agency group, the Activity column of the audit trail will show the group name and agency (instead of listing each member of the group).
- **GROUP AUDIT TRAIL** – The Group Audit Trail allows administrators to monitor the activity of groups within Axon Evidence and logs actions such as creating a group, adding or removing users from a group, changing permissions of a group, etc.
- **DEVICE AUDIT TRAIL** – The Device Audit Trail shows events, actions, and changes for the selected camera. The audit information can be filtered to a particular date range or show the entire life of the camera. The Device Audit Trail can be used to audit actions performed on video while the file is still on the device (prior to upload). The audit information is available in both PDF and comma-separated values (CSV) format, with each event, action, or change shown on a different line in the audit trail.
- **AXON RESPOND AUDIT TRAIL** – The Axon Respond audit trail consolidates all Axon Respond information, such as which users accessed the Axon Respond map or a livestream, into a single audit trail.

12. Ability for video management administrator to assign different access roles based on user's assignment.

Yes. Axon Evidence supports role-based authentication and authorization. Each user is assigned a role, which determines user permissions, which control levels of access to features and functions in Axon Evidence.

13. Users must be able to attach data to the videos in the field. Data is used to make videos searchable.



Yes. Users in the field can attach data to a recorded video and make them searchable using Axon View. Axon View is a free mobile application (available for both Android and iOS devices) is installed on a smart device and paired to a body-worn camera via a Bluetooth and Wi-Fi connection. Using a smartphone or tablet, users can add metadata to videos from the field. For security purposes, data is not stored on the smart device and cannot be deleted, altered, or edited.

When offload is initiated, the videos stored on the camera will upload to Axon Evidence with the tag information applied from the Axon View application, which can later be used to search for the file.

Officers can tag videos with the following metadata fields:

- **ID** – Case ID of the incident
- **TITLE** – Titles default to the device type, date, and time of the video captured, *e.g.,* Axon Body 3 Video 2012-10-13 1447; this field can be updated by the user at the time of capture to display a more specific title, *e.g.,* suspect name or address of incident
- **CATEGORY** – Allows searching for any category type or to specify any category added by SDPD, *e.g.,* traffic violation or felony arrest. Users can add multiple categories to a given piece of evidence, and Axon View pulls the pre-defined categories and retention criteria from SDPD's Axon Evidence account.

14. System must be capable of accepting photos in addition to videos.

Yes. San Diego PD can ingest and store video, photos, files, and data from other mediums and store them independently or group them around a larger case. When you import an evidence file, Axon Evidence classifies the file by its file-type extension, such as .jpg, .mp3, and .docx. You can filter evidence searches by file type. If Axon Evidence does not recognize a file extension, it classifies the file as "Other."

PHOTOS

You can upload and store virtually any photo file type in Axon Evidence; you can view and edit ARW, BMP, CRW, DNG, GIF, HEIC, JPEG, JPG, NRW, ORF, RAF, SR2, SRF, TIF, TIFF files and RAW image extensions like NEF, CR2, and CR3 within the application. Photo editing tools for cropping, rotating, adjusting brightness and contrasts can be used on these file formats as well. Photos are exported from Axon Evidence in the format in which they were uploaded. For example, if the original photo evidence is uploaded as a JPEG, it will be downloaded from Axon Evidence as a JPEG.

15. System must have file and case sharing capabilities.

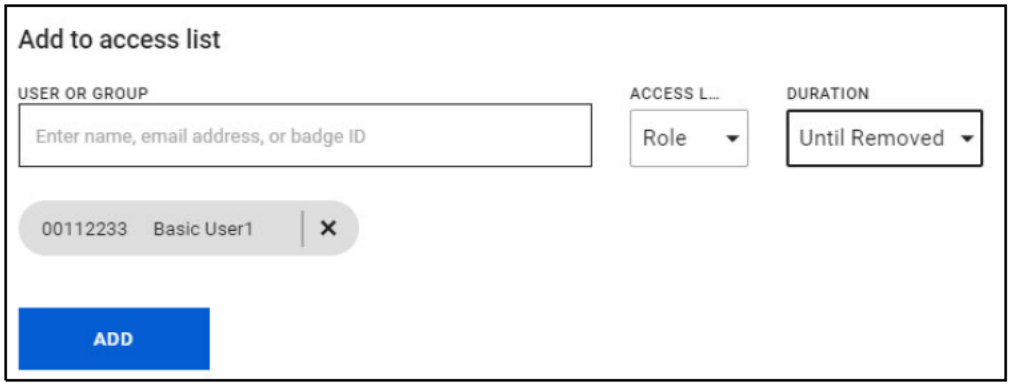
Yes. Axon Evidence provides the following methods for sharing evidence files, each allowed or prohibited by separate permission, enabling administrators to closely control access.

Access Lists control internal and external user access to evidence in Axon Evidence. Each piece of evidence has an access list, so you can individually manage access as needed. If the recipient with whom you wish to share evidence via an external access link does not have an Axon Evidence account, they will receive an email with a link to create an account. An account must be created to preserve the chain of custody.

When adding a user to the access list for a piece of evidence, Axon Evidence allows a user to set the:

- **SHARING DURATION** – Amount of time a user has access to the evidence
- **ACCESS LEVEL** – Level of access to evidence for the selected users

Once the duration and access level are selected, an email is sent to each user informing them they have been added to the access list for the selected files.



Access Lists also control access to Axon Evidence by users outside your agency. This is particularly useful for FOIA and public records requests, as well as sharing files with prosecutors and public defenders. You can share evidence with external users and any Axon Evidence partner agencies.

SHARING WITH PARTNER AGENCIES AND LEGAL PARTNERS

Since these external users already have Axon Evidence credentials, accessing the evidence shared is as easy as logging into the application. After you have added the evidence, you share the case with the trusted partner agencies that you choose.

CASES

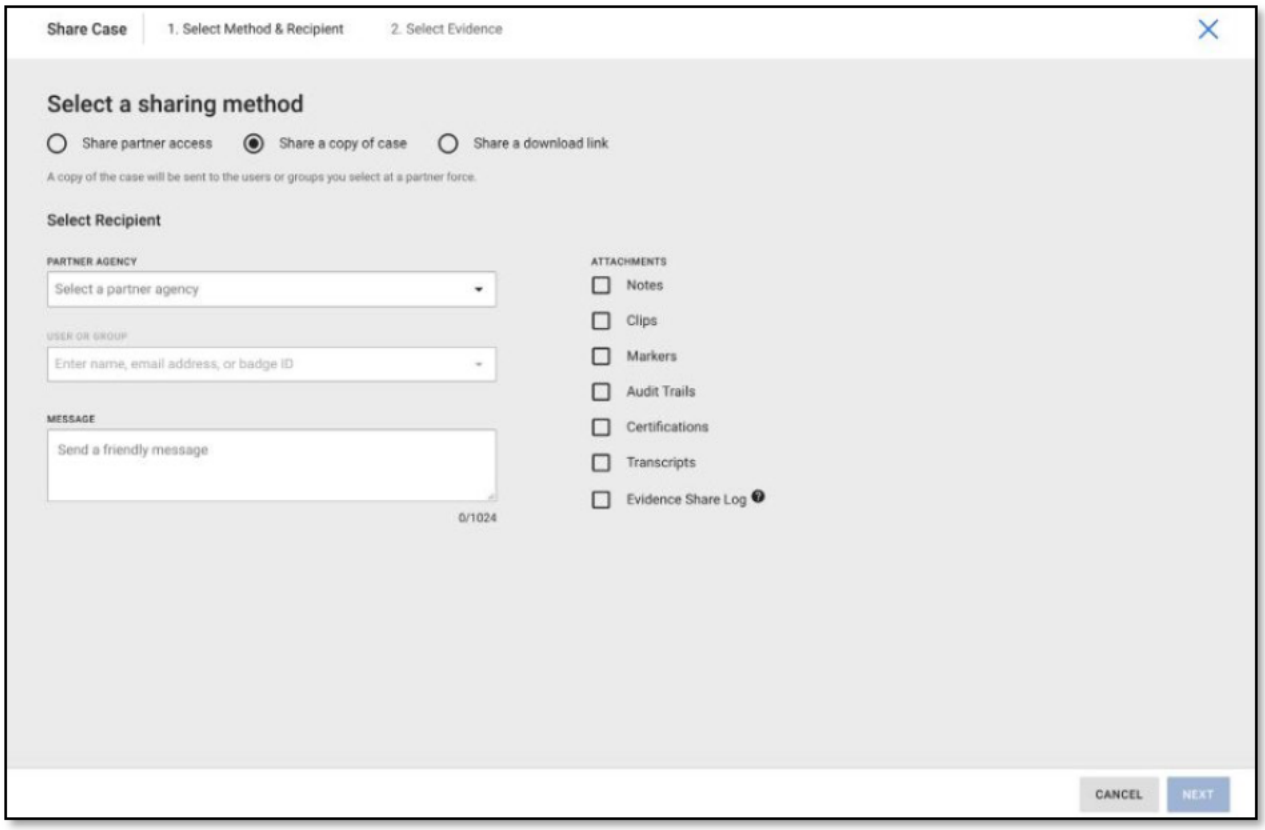
The Axon Evidence Cases functionality allows authorized users to group pieces of evidence to be reviewed, shared, and managed from one central location. The feature has been thoughtfully designed to help users limit time spent gathering evidence, share groups of evidence both within and outside of an agency, and easily search within a subset of evidence files. Additionally, all actions associated with the case and its files are captured within the accompanying Audit Log to protect the chain of custody.

SHARING CASES EXTERNALLY

By clicking the **Manage Shares** button on the main case page, cases can be shared with an external agency. Cases can also be shared via an email address. These two sharing methods offer simple workflows when sharing evidence with another law enforcement agency, a district attorney, or when fulfilling a FOIA request.

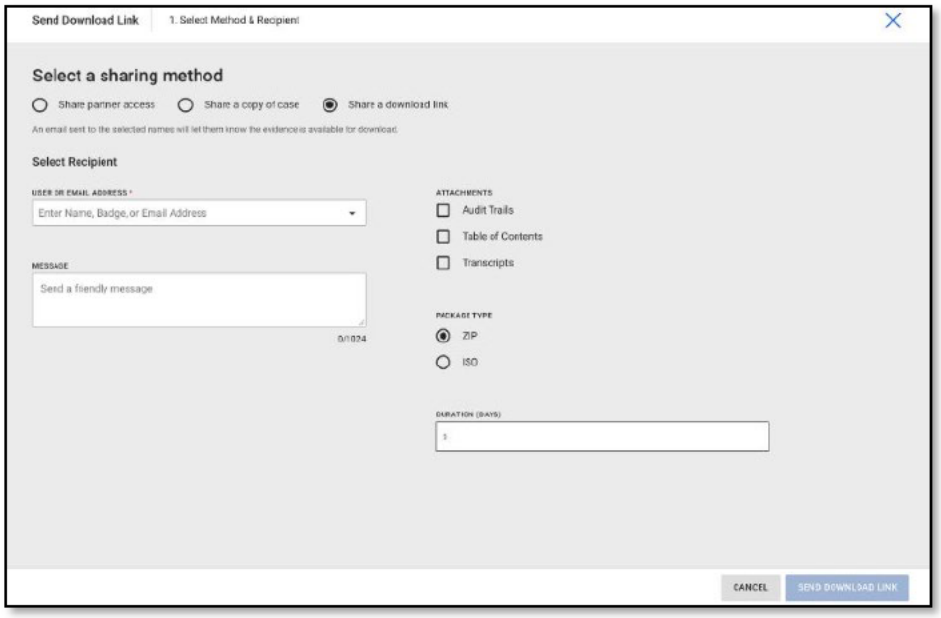
SHARE WITH A PARTNER AGENCY

Sharing with a partner agency creates a copy of the case in the partner agency's instance of Axon Evidence. Attachments (notes, clips, markers, audit trails, transcripts) can be shared, a message can be added, and the share is entirely customizable—a user can choose to share all evidence associated with the case or only select pieces of evidence. Once evidence is selected and the share is initiated, the system will indicate that the case has been successfully initiated for sharing. The recipient will receive an email once the case is copied to their account. Additionally, if new evidence is added to the case, the share can be updated to include the new evidence.



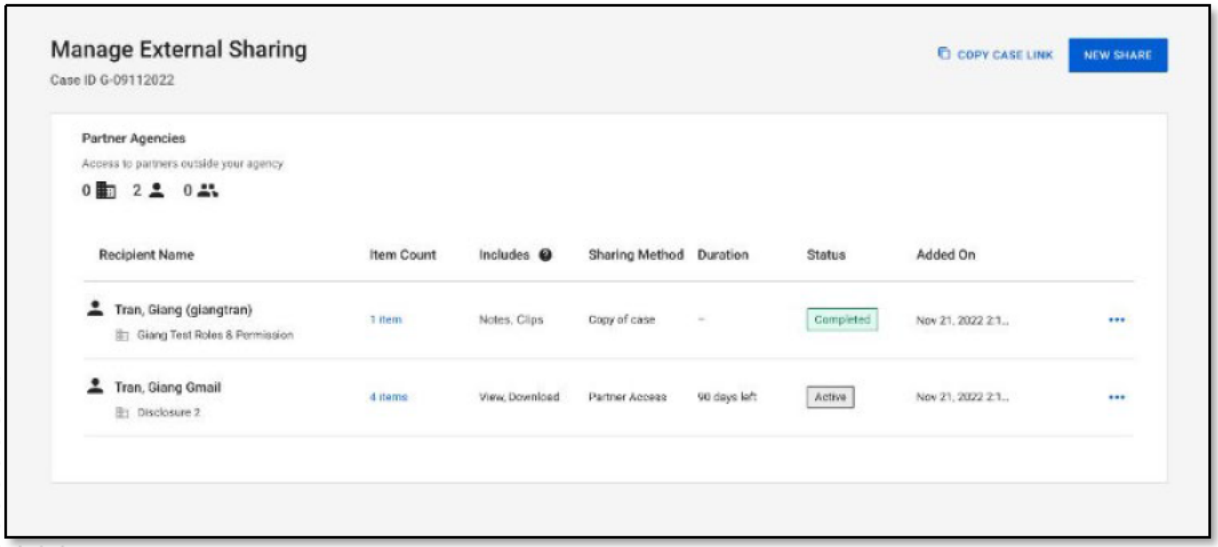
SEND A DOWNLOAD LINK

Download packages can be shared with users in your agency, with a partner agency, or by entering an email address. These packages are available in both ZIP and ISO formats. Users can include audit trails, a table of contents, transcripts, and a message in the package, and set the duration that the evidence link will be available to the recipient. Please note that with this sharing method, the download link can be used by anyone who receives it.



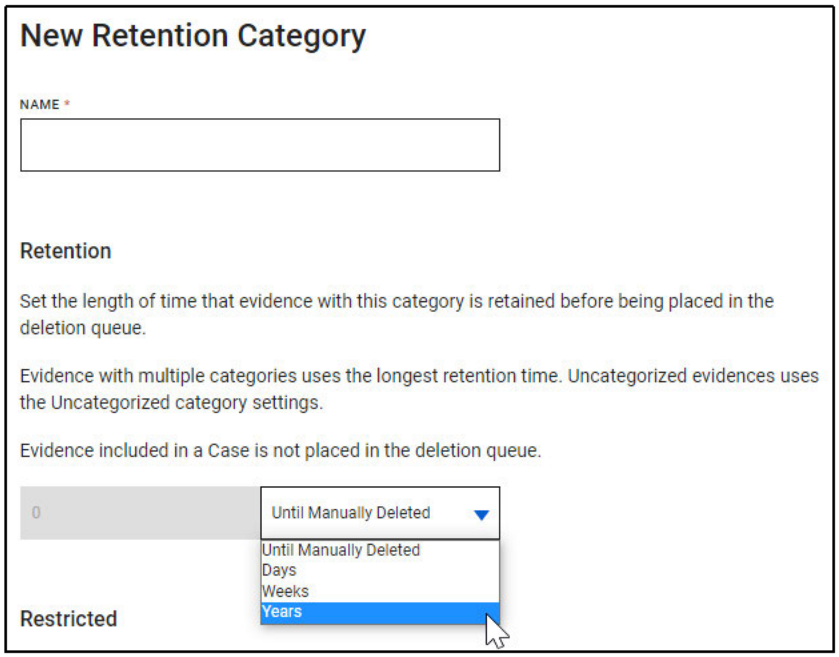
TRACKING ACCESS

After a case is shared successfully, the details are displayed in the **Manage External Sharing** table. Please note that information on case download shares is not currently included in the table.



16. Ability for automatic file deletion schedules in addition to the ability of the administrator to change the preset schedules.

Yes. Axon Evidence administrators can create custom retention categories that determine how long a piece of evidence remains in the system before being permanently deleted. Administrators simply assign a name to indicate the charge (burglary, assault, homicide, etc.) and the desired retention period—determined by policy or state mandate—in days, weeks, years, or until manually deleted. An administrator can create an unlimited number of custom categories and will always be able to edit or delete a category after it is added to the system.



Once created, a user can then begin assigning custom retention categories to any piece of evidence they have access to. When assigned to a piece of evidence, categories not only associate an agency's desired retention period to the file, but they also help to improve search functionality, reporting capabilities, and overall access control.

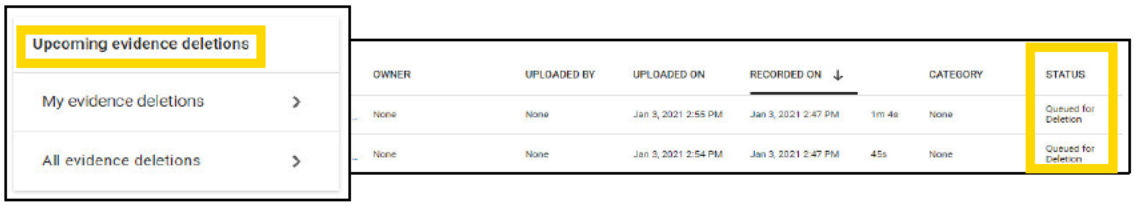
Additionally, if a piece of evidence falls under multiple incidents, *e.g.*, assault and burglary, more than one category can be assigned to the file. That file will then take on the retention period of the category with the longest duration.

At the end of a file's retention duration, Axon Evidence will initiate an automatic deletion process that includes notifications, a grace period for recovery, and restoration options. This process can help agencies manage file storage and prevent inadvertent data loss. Alternatively, evidence can also be manually deleted by authorized users, but no matter if a file is deleted by automatic or manual means, it will remain in a system queue for seven days after being marked for deletion, thus allowing the files to be retrieved if inadvertently removed.

When setting retention durations, Axon encourages agencies to reference state retention schedules or consult with prosecuting partners or other legal counsel for guidance.

REVIEWING UPCOMING EVIDENCE DELETIONS

When a piece of evidence finally hits the retention duration set forth by the category, the system will notify the owner of the evidence via email. The owner can then sign in to Axon Evidence and view their upcoming evidence deletions from the Axon Evidence Dashboard.



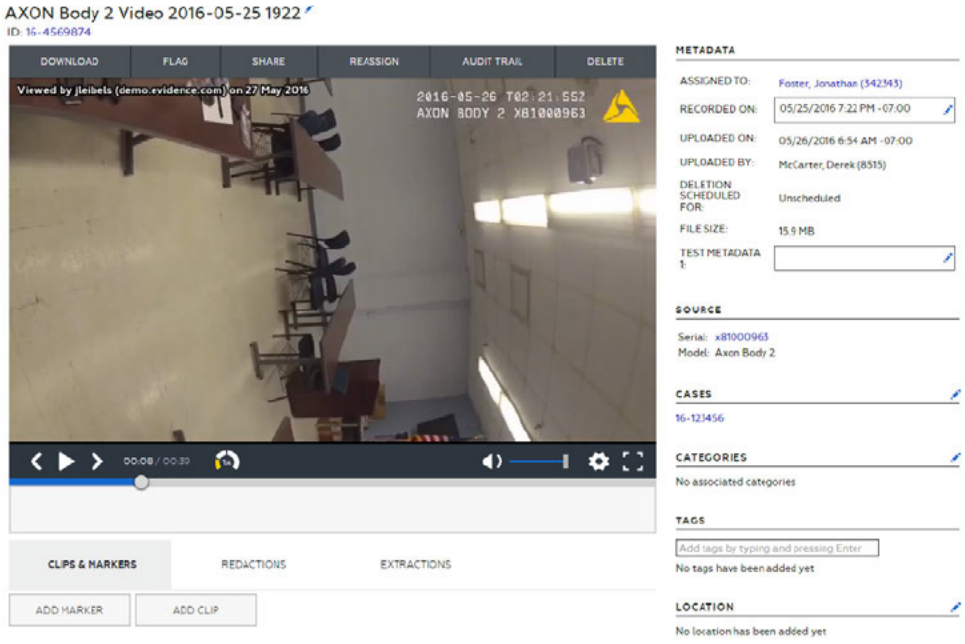
Please note that all evidence audit trails will be preserved, even after the file is removed from the system.

17. Videos should be watermarked for security purposes.

Yes. All Axon videos feature an embedded visual watermark containing metadata (displayed at the top of the video). Metadata fields displayed as a watermark (or overlay) during playback include:

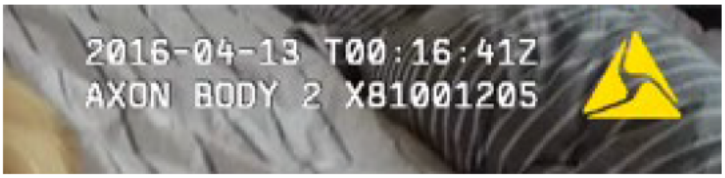
- **VIEWED BY** – (Username – Agency Axon Evidence Account)
- **DATE VIEWED** – (Day/Month/Year)
- **DATE AND TIME RECORDED** – (yyyy/mm/dd - hrs:mins:secs GMT)
- **CAMERA MODEL** – (Axon Body, Axon Body 2, Axon Flex)
- **CAMERA SERIAL NUMBER** – (i.e. X8000000)

Additional metadata fields are displayed on the right-hand side of the Axon Evidence player.



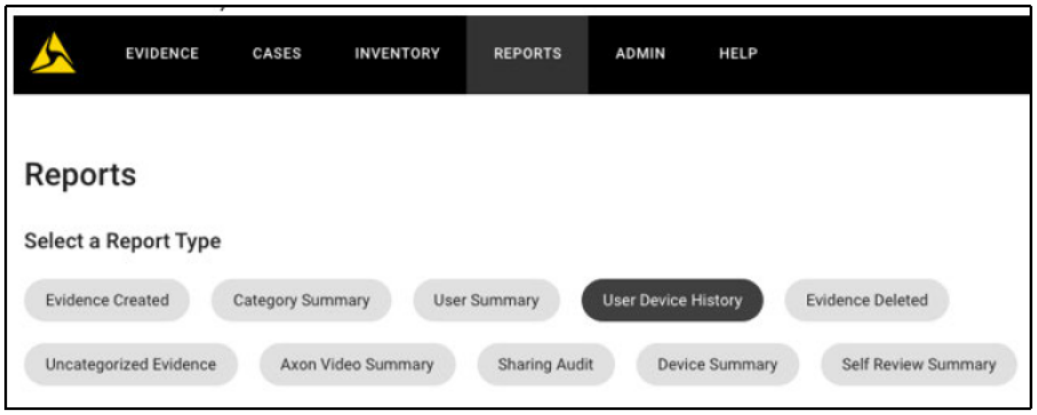
SDPD can turn on/off a permanent watermark (metadata overlay). This information is embedded into the video at the time of recording and will remain visible on the video when viewing, exporting, or sharing. These include:

- Date
- Time
- Type of Device
- Device ID



18. Ability for customizable reports/logs.

Yes. Axon Evidence gives users the option to export standard reports generated as .XLSX files. When generating a report, users can select a specific date range to only include information in the desired timeframe.



These reports include:

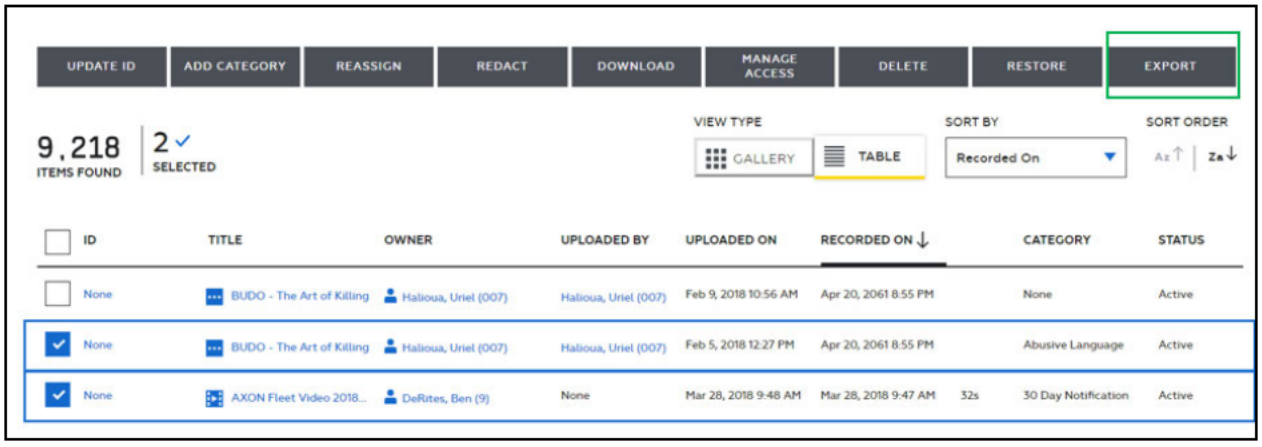
- **EVIDENCE CREATED** – Includes information on when data was created, associated metadata, the number of days between when a piece of evidence was recorded and/or uploaded, and what evidence has been shared through access controls.
- **CATEGORY SUMMARY** – Includes information on the current total file count, file sizes in megabytes (MB) for each category, and the percent of files assigned to a category.
- **USER SUMMARY** – Includes information on a user's total number of files (by file size in MBs)—whether active or deleted—Last Login Date, Invited Date, and Deactivated Date.
- **USER DEVICE HISTORY** – Includes information on devices (TASER energy weapon products and body-worn cameras) assigned to or unassigned from a user during a specific date range.

- **EVIDENCE DELETED** – Includes information on all deleted evidence, associated metadata, and the number of days between when a piece of evidence was recorded and/or uploaded.
- **UNCATEGORIZED EVIDENCE** – Includes information on users with uncategorized evidence assigned to them, as well as owner information, evidence titles, dates recorded, and links to the evidence.
- **AXON VIDEO SUMMARY** – Includes information on usage metrics of videos uploaded to your agency, as well as the number of videos, hours, and MBs.
- **SHARING AUDIT REPORT** – Includes information on a user's actions when sharing evidence and cases.
- **DEVICE SUMMARY REPORT** – Includes information on the devices belonging to an agency.
- **SELF REVIEW SUMMARY** – Includes a list of coach requests that have been sent for additional video review

EXPORTING EVIDENCE, CASE, AND DEVICE SEARCH RESULTS

In addition to the standard reports available in Axon Evidence, agencies can also export the results of a search in PDF, Microsoft Excel, text, or CSV format.

Simply search for evidence or case and refine the search until the results represent the evidence list that you want to export. Check the ID box for all applicable files and click export as shown in the following screenshot. If the search results contain more than 500 evidence files, Axon Evidence provides the list in 500-file segments and asks you to confirm the download of the next segment.



The results are populated in a list and can be exported in a PDF, text, or Microsoft Excel/CSV format.

CUSTOMIZED REPORTS

Authorized users can customize the standard Axon Evidence reports by using Microsoft Excel or other spreadsheet applications to filter report results. If API services are enabled and configured, system administrators can use the Reports API to retrieve report data, which can then be provided to other applications or systems as needed for filtering and analysis. For example, the report data that is retrieved from the Reports API can be sent to a Tableau instance, Microsoft Excel, or a local database.

AUDIT LOGS

Detailed audit logs track all evidence access and activity. Each audit trail entry shows the date, time, user, and details of each action. You can view the entire audit log or a portion of an audit trail, limiting the report to actions that occurred between a specified timeframe. Audit trails are available in PDF format, except the user audit trail and device audit trail, which are available in both PDF and comma-separated values (CSV) format.

- **AGENCY AUDIT TRAIL** – The agency audit trail shows agency-wide changes to your Axon Evidence account. This report helps provide transparency on administrative actions across Axon Evidence. By displaying each action in detail, your agency can review who changed a setting, to understand the purpose and provide better accountability to each user. Only users with the "Edit Agency Settings permission" enabled can view the Agency Audit Trail.
- **AXON RESPOND AUDIT TRAIL** – The axon respond audit trail consolidates all Axon Respond information, such as which users accessed the Axon Respond map or a livestream, into a single audit trail.
- **CASE AUDIT LOG** – The case audit log shows what updates were made to a case and when, including when tags were added or removed. You can export a PDF with the entire audit trail, or with information about a specific date range.
- **DEVICE AUDIT TRAIL** – The device audit trail shows events, actions, and changes for the selected camera. The audit information can be filtered to a particular date range or show the entire life of the camera. The Device Audit Trail can be used to audit actions performed on video while the file is still on the device (prior to upload). The audit information is available in both PDF and comma-separated values (CSV) format, with each event, action, or change shown on a different line in the audit trail.
- **EVIDENCE AUDIT TRAIL** – The evidence audit trail shows all related actions to a single piece of evidence, as well as any associated metadata. All changes made to videos and associated metadata—including, but not limited to, reassigning a video, sharing a video, renaming a video, redactions, and deletions—are logged in the evidence audit trail, including information about the date, time, and user who made the change. The original data associated with a video is never changed; all modifications are handled by creating new, derivative files. To ensure chain of custody, evidentiary files can be verified for authenticity by matching the SHA-2 hash of the original file ingested in Axon Evidence to that of any copy created.

- **GROUP AUDIT TRAIL** – The group audit trail allows administrators to monitor the activity of groups within Axon Evidence and logs actions such as creating a group, adding or removing users from a group, changing permissions of a group, etc.
- **USER AUDIT TRAIL** – A user audit trail shows many of the activities performed by the user, changes to the user account, and evidence-related user actions. In addition to evidence-related user actions, the User Audit Trail will show failed login attempts, when a user is locked out of their account due to multiple failed login attempts or when a user's password has been reset or their account has been unlocked.

19. System must be capable of allowing victims/witnesses/citizens to upload videos at the request of investigators.

Yes. Yes. The system allows victims/witnesses/citizens to upload videos at the request of investigators. Axon Citizen makes it easy for members of the public to submit photos, videos, and other digital files related to an incident, and for your agency to manage that content in Axon Evidence. This technology-based collaboration between law enforcement agencies and the citizens they serve will support community relations and help lead to more informed and successful prosecutions.

Axon Citizen consists of two services—Axon Citizen for Officers and Axon Citizen for Communities. Axon Citizen for Officers facilitates one-on-one officer evidence collection from witnesses in the field, typically via smart devices. Axon Citizen for Communities allows agencies to solicit and collect evidence from the community at large through secure public portals.

With Citizen for Officers, users issue individual invitations via text or email containing links that witnesses can use to upload potential evidence files. With Citizen for Communities, agencies set up and announce public portals through which community members can request text links to submit files to the agency.

All submissions are scanned for viruses and then go straight into Axon Evidence with your agency's other files, eliminating any need to download, print, or transfer content to a USB drive, and submit it to the evidence locker. All submissions will be automatically categorized and searchable within Axon Evidence to simplify case building.

Axon Citizen's triage tool in Axon Evidence allows the officer reviewing submissions to decide which content to accept or decline quickly.

AXON CITIZEN FOR OFFICERS - ONE-ON-ONE EVIDENCE COLLECTION

When you are responding on the scene, you shouldn't have to worry about the chain of evidence when collecting potential evidence from witnesses. With Axon Citizen for Officers, you can invite witnesses to securely send digital files through the Axon Capture mobile application or Axon Evidence on your MDT. Once collected, their submissions go straight into Axon Evidence and are immediately logged in the audit trail instead of sitting on your camera roll or in your email.



AXON CITIZEN FOR COMMUNITIES; COMMUNITY-WIDE EVIDENCE COLLECTION

You always want help from the community, but you don't want to be overwhelmed. Axon Citizen for Communities simplifies the collection process, letting you create portals where community members can request secure links to upload potential evidence files. Then, your agency can review the content as fast as possible to accept or reject submissions. All submissions are instantly categorized and searchable.



Aside from providing a secure way to collect these submissions, a major benefit to agencies is that everything collected through Axon Citizen is integrated into Axon Evidence. All the other Axon Evidence features like search, audit trails, and retention work as you'd expect. Axon Citizen utilizes Axon Evidence's secure audit trail to show which officer initiated the evidence collection, for which incident, at what time and place, and from which community member.

AXON CITIZEN FEATURES & BENEFITS

- **CENTRALIZES YOUR EVIDENCE** – Media goes straight into Axon Evidence with your agency's other files, eliminating any need to download media, print, or transfer it to a USB drive, and submit it to the evidence locker.
- **PROTECTS THE CHAIN OF CUSTODY** – Axon Citizen utilizes Axon Evidence's secure audit trail to show which officer initiated the collection, for which incident, at what time and place, and from which community member.
- **ACCELERATES THE REVIEW PROCESS** – Axon Citizen's triage tool allows the officer reviewing submissions to decide which submissions to accept or decline quickly.
- **STREAMLINES SEARCHING** – All submissions will be automatically categorized and searchable within Axon Evidence to simplify case building.
- **ACCEPTS ANONYMOUS SUBMISSIONS** – Community members may submit anonymously, helping agencies reach individuals who otherwise would not submit evidence.
- **OFFERS NETWORK RELIABILITY** – Axon Citizen manages all the infrastructure and tools needed to support large volumes of submissions, so your agency can remain confident that the service will work during large-scale events.

9. ADDITIONAL AVAILABLE FEATURES

The proposer must have the following additional add-on features available for purchase by the City:

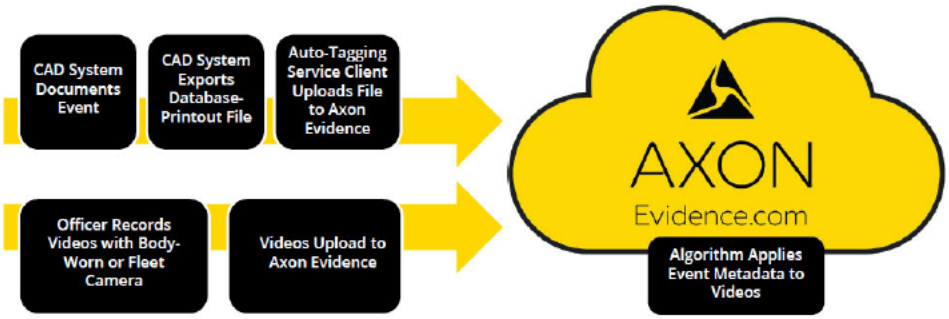
1. **Ability for event data to automatically be added to each video based on integration with City's CAD vendor Hexagon (auto tagging).**

Yes. Axon's Auto-Tagging service allows SDPD to leverage metadata from its Hexagon CAD solution to efficiently manage video-evidence files within Axon Evidence. To do so, the Axon Auto-Tagging service automates the extraction of critical metadata from the CAD software and adds that metadata—which can include ID, retention category, and event location information —to officer recorded video-evidence files in Axon Evidence. The process includes:



USER EXPERIENCE AND DAILY OPERATIONS

After the Axon Auto-Tagging Service is fully implemented, your officers will no longer need to manually add metadata to your evidence files. They simply record videos with Axon body-worn or in-car cameras, upload those videos, and relevant metadata from your CAD and RMS solutions will be applied via Axon Evidence.



When videos are uploaded to your instance of Axon Evidence, videos become managed video-evidence files. The next time your systems place a generated database-printout file in the metadata-export folder, the Auto-Tagging Service Client uploads the file to Axon Evidence.

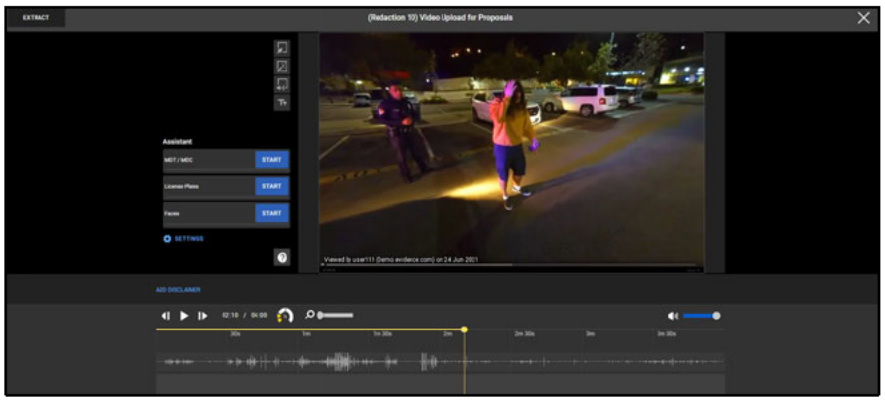
When Axon Evidence processes the metadata in the database-printout file, it uses SDPD's custom algorithm to determine which video-evidence files to tag with the metadata.

2. Video redaction capabilities to include audio and video.

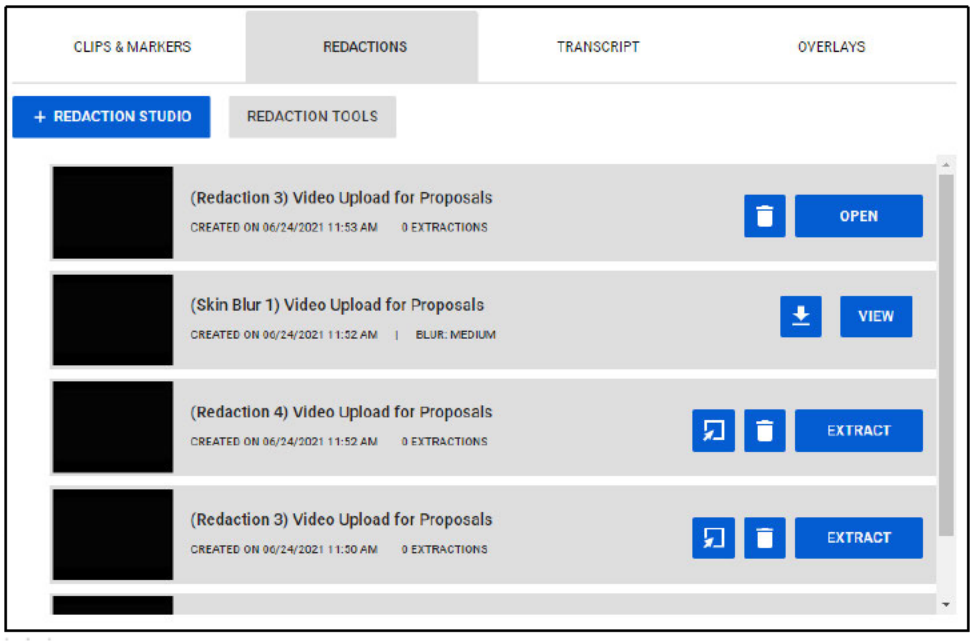
Yes. Within Axon Evidence, users can leverage our built-in redaction suite—which includes our full-featured Redaction Studio, automatic Redaction Assistant tools, and basic redaction capabilities—directly from the cloud.



Redaction Studio allows users to review, playback, and redact an evidence file, as well as utilize redactions and annotation tools to determine what can be seen and heard when viewing a video or image.



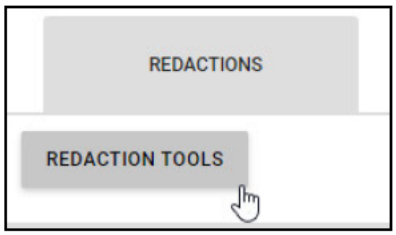
As changes are made and redactions are created, Axon Evidence never alters an original evidence file. Instead, the system generates a list of each redaction associated with the evidence file, which can be accessed from the Redaction tab under the media player on the Evidence Details page. As multiple redactions are made, this list can help users easily access their redactions and ensure evidence integrity is maintained.

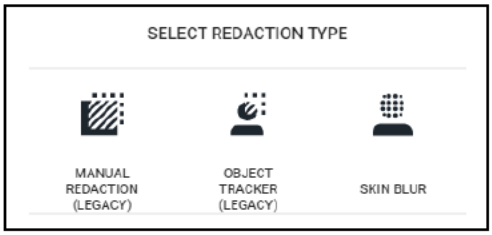


With proper permissions and licenses, users can either manually redact evidence with precision using the Redaction Studio or utilize automated Redaction Assistant tools to expedite the redaction process. These tools include:

BASIC REDACTION TOOLS

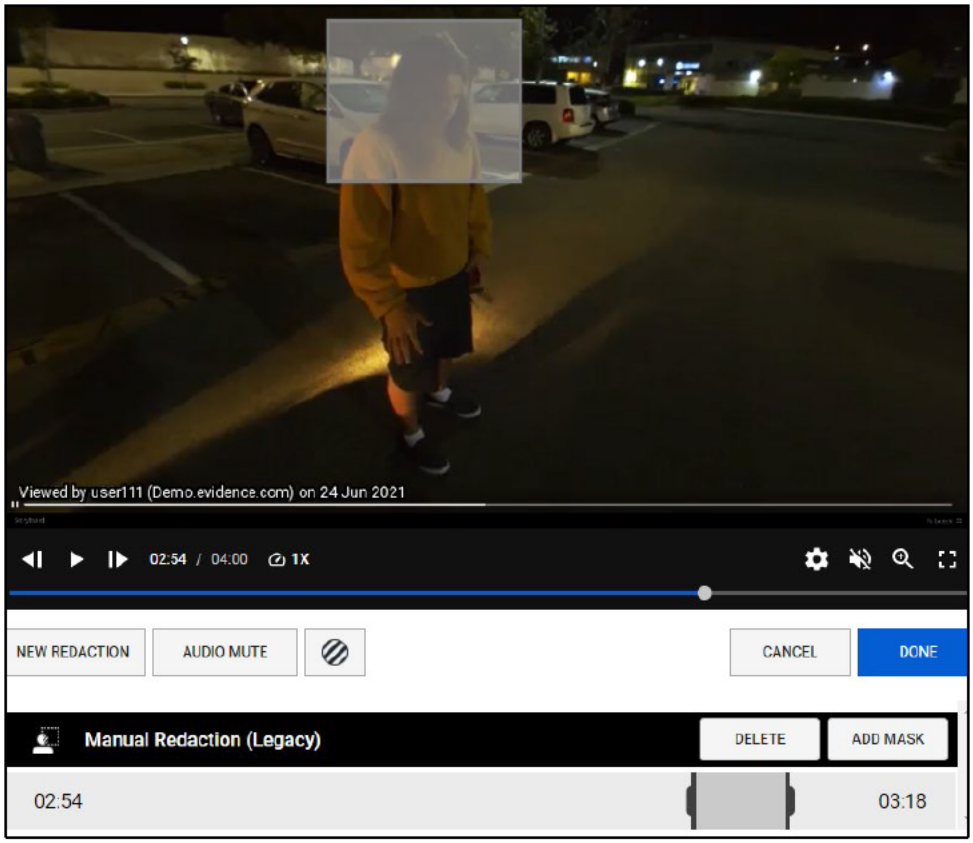
By using the Basic Redaction tools from the Evidence Details page, users can automatically generate the following redactions.





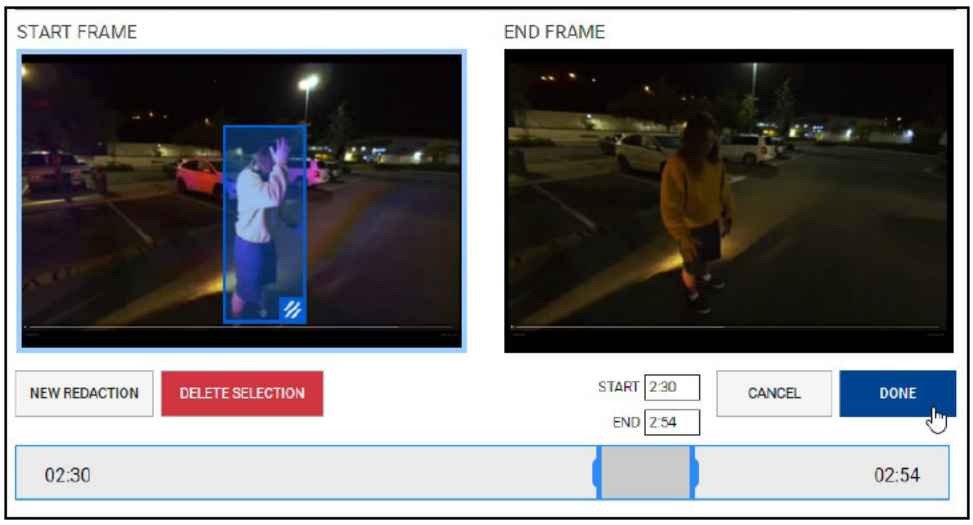
MANUAL REDACTION

The Manual Redaction tool will automatically apply static masks to a video with precision and accuracy.



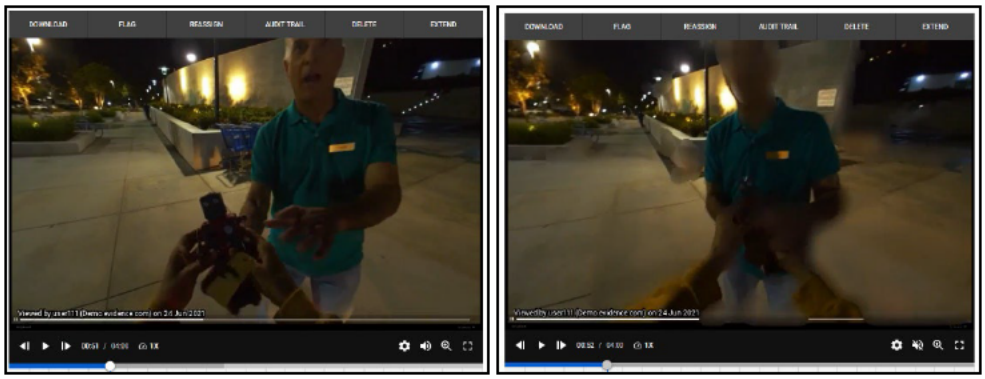
OBJECT TRACKER

The Object Tracker tool allows users to set a frame around objects in the video for the system to automatically track and redact.



SKIN BLUR REDACTION

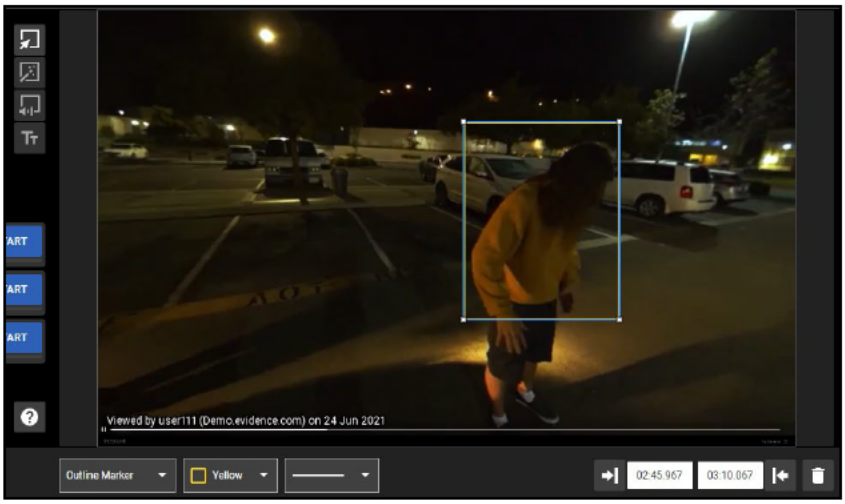
The Skin Blur tool allows users to set a frame around a person in a video so that the system can automatically search for and blur skin tones throughout the entirety of the video.



REDACTION STUDIO TOOLS

MANUAL MASK

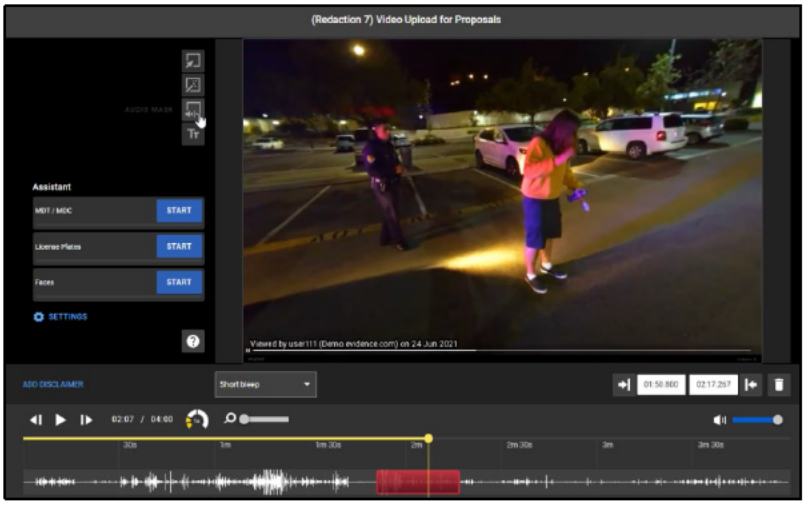
The Manual Mask or Frame-by-Frame Manual Redaction tool allows users to add a mask or outline marker to a video whether it is paused or being plated. This allows users to apply masks and outline markers to specific frames throughout the video, each of which can be extracted as a redaction.



Additionally, a user can click, drag, and resize each mask and outline marker as the video plays, which gives the user more granular control as an object moves about the frame. At Axon, this manual process is referred to as using the Spray Paint tool because users can place a manual mask covering over the desired object, click and hold on the mask, and then use the mouse to follow the object they want to redact.

AUDIO MASK

The Audio Mask tool allows users to hover over portions of audio they would like to mute, and by clicking in the waveform region, an audio mask can be placed. To extend an audio mask, a user simply clicks and drags the end of the segment they wish to adjust or they can enter the time inputs.

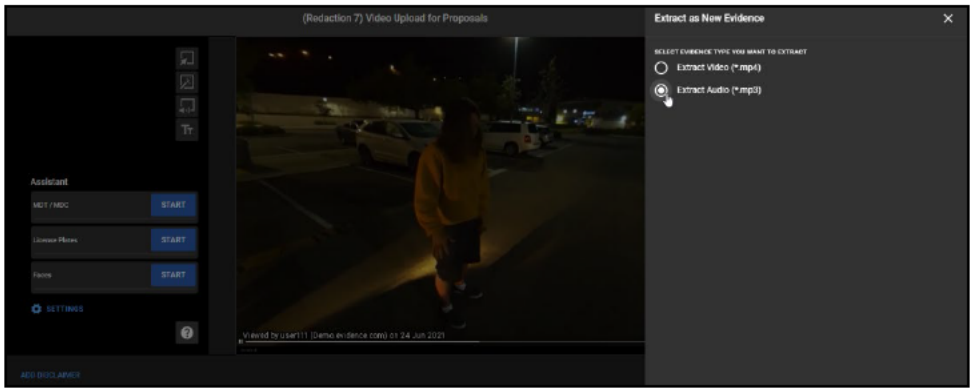


Additionally, users have the option to add a short bleep to a section of video where audio has been redacted. This beep can help viewers identify where and when audio has been muted in the video.



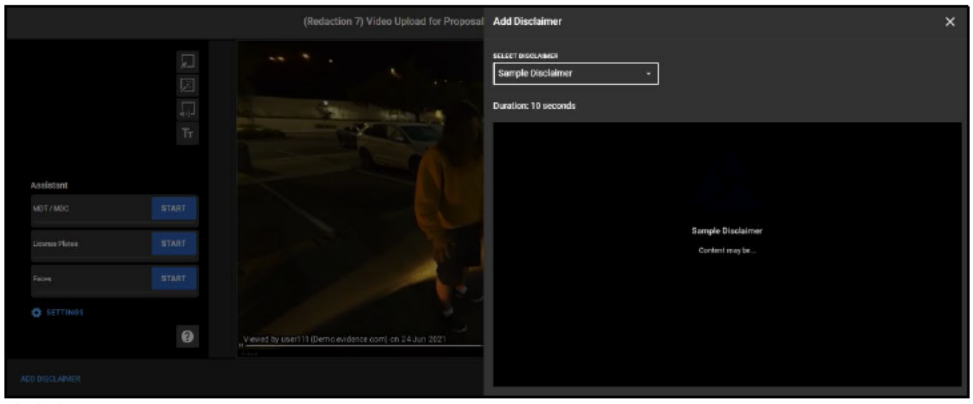
EXTRACT AUDIO

The Extract Audio option allows users to extract the audio track from a video file in an .mp3 format. This is especially useful when combining this option with the Audio Mask tool. By using the two, a user can redact audio from an evidence file, and then extract that redacted audio without video, thus adding an extra layer of privacy and reducing overall file size.



ADD DISCLAIMER

The Add Disclaimer tool allows users to select and add an agency-defined disclaimer from a drop-down list within Redaction Studio, which adds a disclaimer to the beginning of a redacted video file. This disclaimer can be used to warn viewers of violent or disturbing content.



REDACT IMAGE

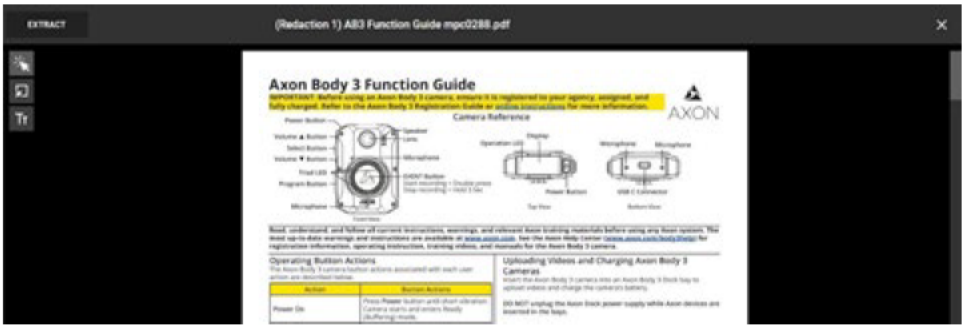
The Redact Image tool allows users to apply a redaction mask to an image file. The workflow for image redaction is similar to using manual masks in Redaction Studio. Users can open the image in Redaction Studio, place masks as needed on the image, and then extract the redaction. Additionally, users can change the mask blur level as needed and rotate the image.

Please note, image redaction is only supported for .jpg and .png file types; support for other file types will be added in future releases.



DOCUMENT REDACTION

The Document Redaction tool allows users to redact text, add masks, and add text annotations to PDF files.

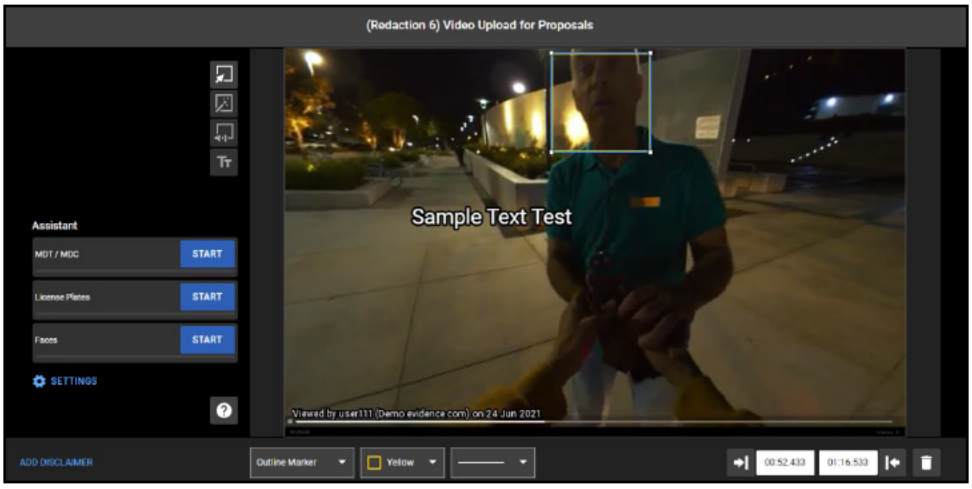


Additionally, agencies with Redaction Assistant enabled will also have access to the search and redact functionality. This allows users to search for keywords in the document and use masks to redact information in bulk. The search feature also supports the navigation of search results to conveniently preview information.

ANNOTATION TOOLS (OUTLINE MARKER AND TEXT TOOL)

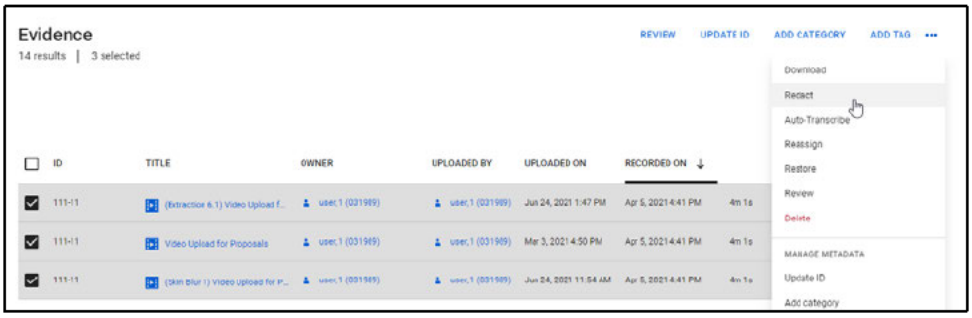
Annotation tools allow users to add outline markers and text to video redactions. The Outline Markers tool can be used to create frames that surround an object in a video to help call attention to a particular object, as well as follow the object as the video progresses. The Text tool allows users to place text in a video, adjust text positioning,

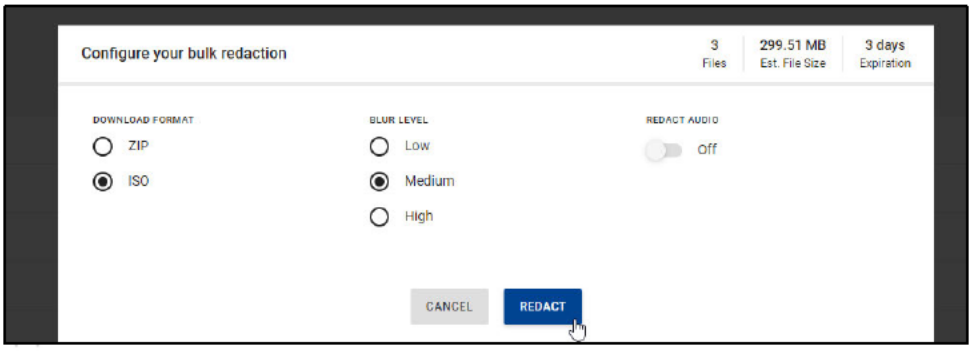
and include text throughout the video. When the redaction is extracted, the outline markers and text boxes will be included in the final file.



BULK REDACTION

From the Evidence Search page, users can select multiple evidence files at once and initiate a bulk redaction. By doing so, users can quickly create copies of the original videos, and the system will automatically apply a blur filter over the entirety of every selected video and remove audio for the duration of the footage if desired. Applying a blanket blur over the entire video helps users preserve privacy and fulfill public disclosure asks, while still providing audio evidence for context.





AUDIO REDACTION VIA AUTO-TRANSCRIBE

The Audio Redaction via Auto-Transcribe feature allows users to quickly identify important moments in evidence to reduce time spent redacting audio. Users can either click on a word or search for a word in the auto-transcript to jump to the point in the video when the word was spoken. Users can also drag their mouse over entire portions of the transcript to highlight phrases, sentences, or large sections of audio. Once the desired words have been selected, a simple double-click or right click will redact the audio from the file.

This feature is compatible with video files or audio-only files.

Note that this feature requires access to Redaction Assistant and Auto-Transcribe. Either unlimited or ala carte Auto-Transcribe minutes can be used.

3. Live feed from multiple cameras that are in record mode.

Yes. Axon Body 3 and Axon Body 4's integration with the Axon Ecosystem enables dispatch and command staff to gain real-time situational awareness of events in the field, through Axon Respond. Axon Respond enables remote personnel to quickly gain insight into a call-for-service or an officer's whereabouts. By simply signing into Axon Evidence or the Axon Respond mobile application, the personnel can open up the Axon Respond Map and access livestreams from active cameras, view location data as cameras move, and receive live alerts and notifications. This includes Watch Me notifications sent from an officer's body-worn camera, which will allow dispatch or command staff to quickly access a livestream and begin bi-directional communication with an officer in need, in real-time, through Axon Respond.

These capabilities make it possible for those not on the scene to gather better intel and help officers in the field as situations change. Whether checking in on a responding officer or sharing tactical advice during a critical event, Axon Respond gives your agency access to information in the moment.

With our Axon Respond+ functionality enabled, an Axon Body camera can livestream from the device to Axon Evidence or the Axon Respond mobile application. A typical Axon Respond + livestreaming workflow may look like this:

- Officer begins recording
- Once recording has been initiated, the supervisor or dispatcher opens the Respond tab in Axon Evidence on their computer, clicks on the officer's marker on the live map, begins live streaming, and can now respond accordingly
- If the officer ends the recording, the livestream ends, or the supervisor can exit the livestream at any time (without ending the recording)

This workflow is dependent upon how permissions and access are configured in Axon Evidence per SDPD's policy.

4. Automatic "on" activation feature.

Yes. Axon supports two different types of auto-activation via Axon Signal Technology and remote-based activation.

Axon Signal is a technology that operates over Bluetooth Low Energy and activates Axon cameras within range via various triggers.

The Axon Signal products we offer today are the Axon Signal Vehicle Unit, Axon Signal Performance Power Magazine, and Axon Signal Sidearm. Whether you're driving your vehicle, using a TASER energy weapon, or drawing a firearm, Axon Signal technology ensures vital footage is captured.

AXON SIGNAL VEHICLE UNIT (ASV)

The Axon Signal Vehicle Unit (ASV) is a device installed in the patrol vehicle that broadcasts a beacon to Axon cameras in range when specific events are reported. The following vehicle triggers will signal the system to begin recording:

CONFIGURABLE TRIGGERS

- Light bar/siren activation
- Removing a weapon from the vehicle rack
- Door sensor

In addition to the ASV, we offer the following Axon Signal products:

AXON SIGNAL PERFORMANCE POWER MAGAZINE (SPPM)

The SPPM is an accessory (battery) for TASER X2 and TASER X26P energy weapons. The TASER 7 energy weapon, Axon's newest TASER energy weapon, has this technology built-in and does not require an accessory. Using Axon Signal technology, the SPPM activates cameras when the TASER 7 energy weapon is armed, the trigger is pulled, or the arc is engaged.

AXON SIGNAL SIDEARM

This easy-to-install smart sensor accessory attaches to the outside of most sidearm holsters and activates if a sidearm is removed from the holster. The action of drawing your weapon will trigger surrounding cameras to start the recording process, thus eliminating manual manipulation. That way, your officers can be confident truth and transparency are being upheld through video and audio documentation.

REMOTE ACTIVATION FEATURE

The Remote Activation feature offers SDPD a dependable and logical integration between your current CAD system and Axon's real-time awareness technology platform, Axon Respond. This remote activation service allows Axon Respond to automatically activate a particular set of Axon Body 3 cameras via CAD activation based on the call for service metadata exported from the CAD system, or when crossing a pre-determined radius placed on the Axon Respond Map.

10. PRICING SCHEDULE

Per the RFP instructions, this information is provided in Tab C – Cost/Price Proposal.

Proposers shall submit their pricing in Attachment 1 of Section C in the following manner:

1. **The Proposer should carefully review this RFP and address all items and services in their proposed fee structure and schedule.**

2. **If a Proposer identifies a package solution(s), the details of what is included in the package (hardware, storage, licensing, etc.) should be listed in the appropriate section of the Pricing Schedule and the cost listed on a per camera basis.**

3. **Unit price will be used to evaluate proposals for pricing in accordance with section 3.6 of Exhibit A of this RFP.**

4. **Award shall be made to a single proposer. Proposer is required to submit pricing for each line item listed in Pricing Pages-Exhibit B, Attachment 1. Proposers may submit additional pricing for Price Schedules and bundles. Pricing Pages-Exhibit B, Attachment 1 will be used to evaluate proposals for pricing in accordance with Section 3.6 of Exhibit A of this RFP. (Other Price Schedules or bundles shall not be included in the evaluation for award)**

5. **Any deviations from the Price Schedule may result in a proposal being rejected as non-responsive. The Pricing Page is the only form and format that will be accepted for proposal pricing.**

6. **Blanks on the pricing pages will be interpreted as zero (0).**

11. TRAINING REQUIREMENTS

1. **All training listed below (2-5) will be provided at no additional cost to the City.**

Yes. Axon will provide the training requested at no additional cost to the City.

2. **Provide on-site instructor certification training for San Diego Police Department Operational Support Administration personnel. If new models of BWCs are released by the successful proposer and purchased by the Department throughout the duration of the proposed contract, the successful proposer shall provide updated instructor certification training for San Diego Police Department Operational Support Administration personnel.**

Yes. Axon will provide on-site instructor certification training for San Diego Police Department Operational Support Administration personnel. If a new model of BWC is released by Axon and purchased by the Department throughout the duration of the proposed contract, Axon will provide updated instructor certification training for San Diego Police Department Operational Support Administration personnel.

3. **Provide on-site training for City and Department technical staff as it relates to video management and storage system specifications.**

Yes. Axon will provide training as described in detail below in response to number 6, on the following page titled Implementation and Training Overview.

4. **San Diego Police Department Operational Support Administration personnel shall be recognized by the successful proposer as certified BWC instructors for the Department.**

Yes. San Diego Police Department Operational Support Administration will be trained by Axon and recognized by Axon as certified BWC instructors for the Department. This initial subset of trainees can act in a "train the trainer" capacity for their co-workers and become a resource when newer users are activated and require training or assistance. They will be trained on body-worn camera functionality, Axon Docks, Axon Evidence, and any applicable mobile applications.

5. **All Department personnel trained by the San Diego Police Operational Support Administration in the use of the BWC shall be recognized by the successful proposer as being properly and sufficiently trained in the use of the BWC.**

Yes. All end users (Department personnel) trained by San Diego Police Operational Support Administration in the use of the BWC will be recognized by Axon as being properly and sufficiently trained in the use of the BWC. End users can be trained one by one or in a train-the-trainer style. Generally, we advise training an initial subset of key end users. The size of this contingency depends on an agency's size or the size of the planned deployment. This group will serve several roles, including confirmation of system functionality, performance, and feedback on any localized issues that had not been previously identified.

6. **All initial training must be completed within 30 days of the execution of the contract.**

Axon will complete training within 30 days of the execution of the contract.

The following Implementation and Training Overview section provides a narrative to provide amplifying detail to our specific responses to requirements 1-6 above.

IMPLEMENTATION AND TRAINING OVERVIEW

Hardware and software features aren't the only things that make a body-worn camera program successful—ease of implementation and the experience of the installation team are just as important. Axon's Professional Services (PSO) packages provide the right training and implementation support to help introduce our technologies to agencies.

To meet the requirements of this solicitation, we are proposing:

- One day of on-site services and remote project planning
- Customizable training, including Administrator, User, and End-User training
- Access to training documentation

This implementation and training overview describes our proposed services, including our Professional Services Organization, our approach to SDPD's project, the details of each phase of the deployment, and a description of the people and services to support SDPD after initial implementation and training is complete.

PARTNERING WITH AN EXPERIENCED TEAM

Axon's Professional Services (PSO) team has extensive experience helping agencies of all sizes implement their body-worn camera programs. By offering dynamic deployment plans, an experienced deployment team, and a solution developed in-house, Axon is uniquely positioned to provide SDPD with a more effective deployment, training, and support experience.

With Axon's staff completing your installation, SDPD can expect project alignment, with end users gaining a more complete picture of the features and functionality of the solution. Our PSO team is authorized to install our proprietary solution, meaning SDPD will benefit from having installers with the most up-to-date product information, product training, and installation techniques.

Many of our PSO implementation specialists joined Axon directly from law enforcement and were responsible for planning and managing similar projects in their former law enforcement roles. This real-world experience is an invaluable resource and allows them to predict and overcome potential challenges as well as effectively collaborate with command and IT staff. Our staff can also offer guidance on custom workflows and processes to help SDPD use your body-worn cameras and DEMS effectively and in compliance with local laws and statutes.

When selecting a solution, it is worth considering whether the hardware and software were built from company acquisitions or developed by the same engineers who support it today. The proposed body-worn camera hardware and DEMS software were designed and maintained by Axon's in-house engineers, allowing our teams to easily pass on feedback or feature requests as your program progresses. Our U.S.-based Technical Support team can engage directly with our in-house engineers for advanced troubleshooting if the need arises. This direct line of communication from system users to developers is something Axon can offer other companies cannot.

AXON'S PROJECT APPROACH

Our team's extensive deployment experience informs Axon's project approach, which is based on the following project management principles.

- **HIGH-QUALITY WORK** – Deliver high-quality end products, address business objectives, and meet end-user requirements
- **ON-TIME DELIVERY** – Complete deliverables on schedule and within budget
- **EFFECTIVE COMMUNICATION** – Communicate in a timely, professional, and detail-oriented manner throughout the entire project
- **EFFICIENT MANAGEMENT** – Leverage team-wide experience to effectively anticipate potential risks, document any complications, and take corrective actions to safeguard project scope, schedule, and budget

Axon believes these principles contribute to the successful management of information technology projects. That is why we consider them when developing our custom project plans and timelines, which are fluid and can be adjusted to fit almost any deployment scenario.

ONGOING QUALITY MANAGEMENT

Axon's project approach uses continuous quality management based on the following quality management principles:

- **VERIFYING QUALITY ASSURANCE** of project deliverables to meet the requirements of the contract.
- **ADDRESSING ISSUES** in a timely and appropriate manner.
- **CONDUCTING PERIODIC PROJECT REVIEWS** to measure compliance with sound project management practices.

Axon's PSO team aims to complete on-time and satisfactory work by considering a proper project approach, working with agencies to develop custom deployment plans, and using ongoing quality management checks throughout the project.

PHASES OF THE PROPOSED PROJECT PLAN

We've built the proposed project plan to reflect lessons learned in our many past successful deployments. To provide the basic structure needed for a body-worn camera deployment, plans are split into three phases:

- **PRE-DEPLOYMENT**
- **DEPLOYMENT**
- **POST-DEPLOYMENT**

Each phase is then further divided into sub-phases, which are made up of individual deployment activities. Each of these sub-phases will be adapted to your specific deployment objectives.

PROJECT PHASE DETAILS

PRE-DEPLOYMENT PHASE

The pre-deployment phase begins once Axon has been selected as your preferred vendor and contract documents have been negotiated and signed. Your account will be handed off to our PSO team, who will begin the deployment planning process. SDPD should determine the main project point of contact from your agency prior to the proceeding steps to help coordinate discussions between SDPD and Axon. This point of contact will work directly with Axon's team to accomplish the tasks necessary for a smooth deployment and training process.

Prior to deployment, SDPD can expect an introductory email and phone call from one of our PSO project coordinators to set expectations for deployment timing and staffing. Administrator guides, networking information, and other critical solution information will be provided to your program point of contact to assist with planning; our PSO team will be available if questions arise.

CUSTOMIZATION OF PROPOSED PROJECT PLAN

During the implementation kick-off, Axon's project manager will adapt the proposed project plan to align with the specific objectives and requirements of your agency. This will allow us to accommodate a wide variety of training, configuration, and timeline requests which will be reflected by changes to tasks within the sub-phases.

The resulting plan will be documented and shared with each member of the team, providing the structure to successfully complete your project implementation. During the final scoping call, the deployment team will also establish that the project plan matches your expectations and the contractually agreed-upon scope. If further training or other services are necessary to complete the project as expected, the project manager will discuss these needs with SDPD.

Axon's PSO team will also evaluate the project for proper scoping and follow-up to obtain additional information if necessary prior to on-site services. This may include information on network specifications/bandwidth, CAD/RMS integration, and other system information that may require involvement from your network administrators or IT team.

DEPLOYMENT PHASE

The proposed Axon Starter package includes one day of on-site services, advanced remote project planning, configuration support, and a professional services manager to work with the SDPD to assess deployment needs and determine if additional on-site services are appropriate. If SDPD requires more than one on-site day, this will be communicated to the sales team for alignment.

CONFIGURATION

The configuration deployment sub-phase includes assistance with hardware installation and software configuration. Axon's PSO staff will assist with the configuration of roles and permissions, custom categories, and other Axon Evidence settings based on the policies you developed in the pre-deployment phase. This coordination is generally done virtually prior to on-site services. Additionally, Axon's PSO staff will assist SDPD personnel with installing, testing, and configuring the body-worn cameras and Axon Dock hardware. Our installation team will note and troubleshoot issues with your IT staff as needed.

TRAINING

Training is entirely customizable to your needs; our experienced PSO team members can train anyone, regardless of their role. Specific topics that are critical for your agency's roles and workflows will be noted, and training on that topic can be delivered. The most common training sessions include:

- **SYSTEM ADMINISTRATOR**
- **USERS**
- **TRAIN-THE-TRAINER**
- **EVIDENCE TECHNICIANS**
- **SUPERVISORS**
- **DETECTIVES**
- **REDACTION TECHNICIANS**

System Administrator training typically consists of a session covering custom roles and permissions, retention categories, and other critical Axon Evidence settings. Additionally, Axon Evidence features will be discussed, including working with evidence, redaction capabilities, case functionality, reporting options, audit trails, and device inventory. Each System Administrator training session is generally three to four hours in length and can accommodate up to 10 users.

End users can be trained one by one or in a train-the-trainer style. Generally, we advise training an initial subset of key end users. The size of this contingency depends on an agency's size or the size of the planned deployment. This group will serve several roles, including confirmation of system functionality, performance, and feedback on any localized issues that had not been previously identified. This initial subset of trainees can act in a "train the trainer" capacity for their co-workers and typically become a resource when newer users are activated and require training or assistance. They will be trained on body-worn camera functionality, Axon Docks, Axon

Evidence, and any applicable mobile applications. Each training session is generally three hours in length and accommodates up to 15 users.

If training for evidence technicians, supervisors, detectives, or redaction technicians is necessary for your program, our team can accommodate you. These sessions are customized and will cover portions of Axon Evidence that are central to the job functions of those in attendance.

GO-LIVE COMPLETE

A post-deployment survey will be sent by the professional services manager after on-site services are complete. This allows SDPD to provide feedback directly to Axon leaders. Acceptance documents also will be sent, and signatures requested. This allows SDPD to officially accept the services as complete or alert our team of any outstanding items. This must be completed within seven days and marks the end of PSO team involvement. Your account will then transition to Axon's post-deployment support team for ongoing program attention.

DEPLOYMENT PHASE SCHEDULE

We have included the following proposed schedule outlining the deployment phase. The final agreed-upon project scope and actual contract award date may affect the deployment tasks and schedule. Please note that some tasks listed in the following table will take place virtually and prior to on-site services. Though tasks may be completed in unison and have different durations, all tasks can be completed within the total days indicated.

SDPD'S PLAN AND SCHEDULE		
CONFIGURATION (5 DAYS TOTAL)		
TASKS	**OWNER**	**DURATION**
Dock Registration and Configuration	Axon, SDPD	1 day
Install and Test Axon Docks	Axon, SDPD	2 days
Create User Accounts in Axon Evidence	Axon, SDPD	2 hours
Inventory, Assign, and Test All Axon Devices	Axon, SDPD	1 day
Create a Video Policy Draft	SDPD	5 days
Record and Upload Test Videos	Axon, SDPD	1 hour
Install Axon Mobile Applications	Axon, SDPD	1 day
TRAINING (1 DAY TOTAL)		
TASKS	**OWNER**	**DURATION**
Administrator Training	Axon	3 hours
Train the Trainer	Axon	3 hours
Evidence Technician Training	Axon	2 hours
GO LIVE COMPLETE (2 HOURS TOTAL)		
TASKS	**OWNER**	**DURATION**
Post-Deployment Meeting	Axon, SDPD	2 hours

POST-DEPLOYMENT

The final portion of the project is the post-deployment segment, which starts after deployment concludes and continues for the life of the solution. Axon is focused on providing dedicated and effective post-deployment support to our customers. We have a full staff of product support and account management specialists in place to help our law enforcement partners have the most successful body-worn camera program possible.

CUSTOMER SUCCESS MANAGER

After the initial deployment, a customer success manager (CSM) will be assigned to your account for the remainder of your contract. Their goal is to support your day-to-day needs, educate you on new features, and help you receive value from your investment. Your CSM will wear multiple hats, from project management to product expert to consultant, and will continually be focused on making SDPD more efficient and confident in your daily workflows. As your program develops and progresses, your CSM can take hardware and software feedback and pass it along to our engineers—another benefit of deploying a solution that is serviced by the same engineers who developed it. In fact, many new features have been built directly from such suggestions from our law enforcement partners. They will also work with your sales executive if any further purchases are desired. Your CSM can be reached by phone or email and will be adaptable to your communication preferences.

TECHNICAL SUPPORT

Our Technical Support team is US-based and offers live phone support 24 hours a day, seven days a week. This is included as part of your investment in the Axon ecosystem and any member of your agency can call; our staff will help anyone with their questions, not just supervisors. Online, email-based support and remote-location troubleshooting are also included.

If a technical issue requires advanced troubleshooting or interfacing with our in-house engineers, our Senior Technical Support team (Tier 2) can take over from the Technical Support team (Tier 1). All senior technical support representatives hold certifications from their respective governments for access to CJI. The team currently holds a variety of education and information technology certifications, and many have a background in law enforcement.

RMA DEPARTMENT

If equipment needs to be returned for repair or warranty work, the process should be as simple and hassle-free as possible. That is why Axon's return material authorization (RMA) request process is housed directly within Axon Evidence, allowing users with appropriate permissions to create repair requests easily. All returns are initiated, tracked, and managed using the hardware's unique device serial number, which also correlates with warranty status and helps protect evidence integrity if evidence recovery is needed. Axon's RMA process is also integrated with FedEx and return labels are provided at no extra cost to be printed by SDPD. Our US-based RMA team works out of our Scottsdale, AZ headquarters and has expertise in Axon's products and solutions.

12. STAFFING PLAN

1. **Qualifications of personnel adequate for requirement.**
2. **Availability/Geographical location of personnel for required tasks**
3. **Clearly defined Roles/Responsibilities of personnel.**

PROPOSED DEPLOYMENT TEAM

Based on the anticipated scope of service and timeline, SDPD can expect the following staff to participate in the deployment process. Each assigned Axon staff member is a specialist in our in-house developed solutions. This means fewer resources are needed to complete your deployment, resulting in a faster and more cost-effective roll-out. Axon will assign an experienced team that includes a(n):

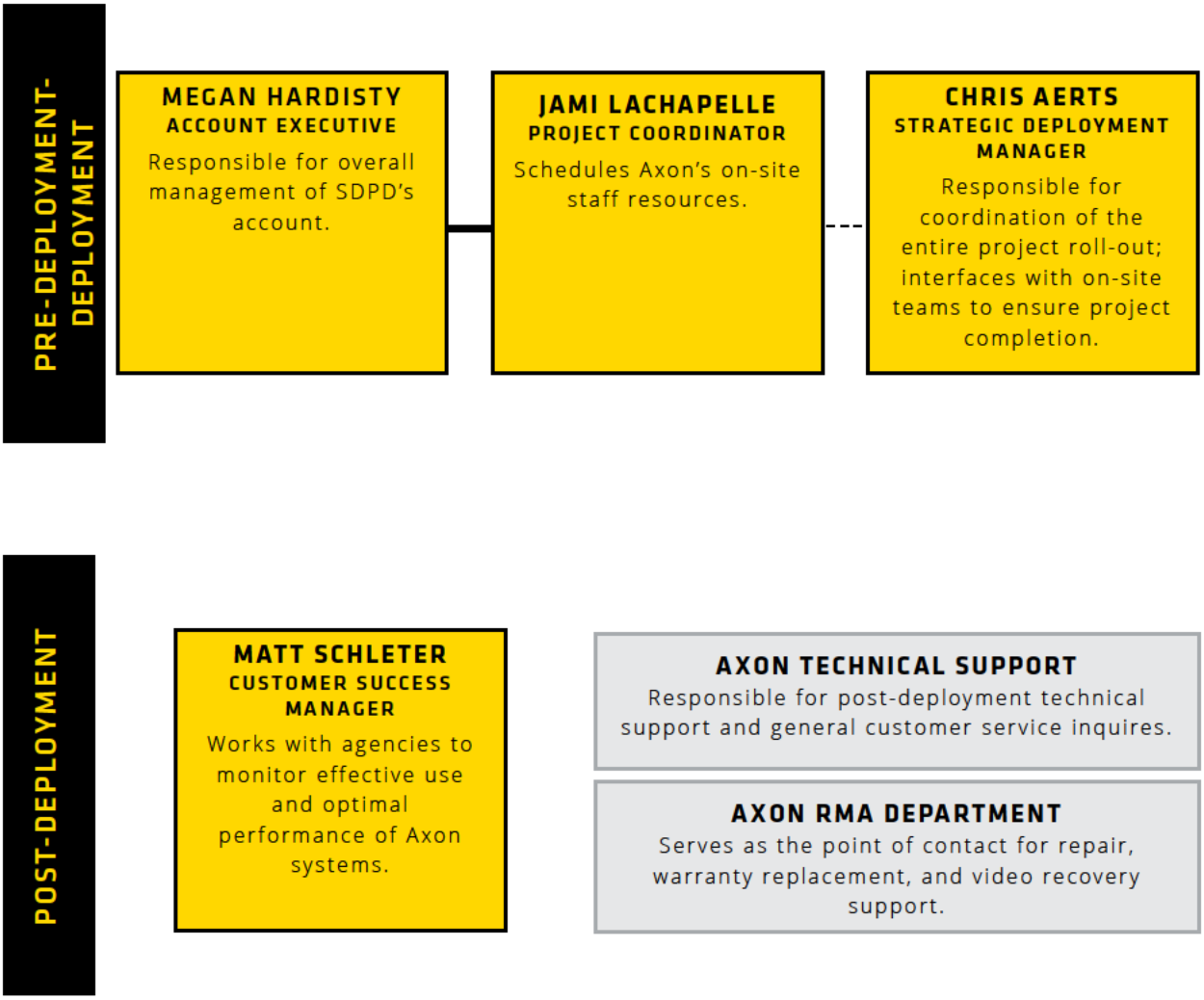
- **MEGAN HARDISTY, ACCOUNT EXECUTIVE** – Responsible for the overall management of SDPD's account.
- **JAMI LACHAPELLE, PROJECT COORDINATOR** – Schedules Axon's on-site staff resources.
  - **CHRIS AERTS, STRATEGIC DEPLOYMENT MANAGER** – Responsible for coordination of the entire project roll-out; interfaces with on-site teams to ensure project completion.
- **MATT SCHLETER, CUSTOMER SUCCESS MANAGER** – Works with agencies to monitor the effective use and optimal performance of Axon systems.

Axon's project team will work directly with the SDPD's project manager to accomplish the tasks necessary for a smooth deployment and training process.

A separate set of staff members will be involved in the pre-deployment, deployment, and post-deployment phases of the project. The pre-deployment team will kick off the process and are responsible for proper project scoping and scheduling prior to deployment activities. Once the pre-deployment activities are complete, the project will be passed to the deployment team, who will complete on-site activities, including any installation and training as agreed upon in the contract. Once on-site activities are complete, your account will transition to the post-deployment phase, and your assigned customer success manager (CSM) will assist with any day-to-day questions you may have. SDPD will also have direct access to our 24/7 Technical Support department as well as DEMS-integrated RMA services.

We have included a project staffing chart and bios for the anticipated team members.

PROJECT STAFFING CHART



PROJECT TEAM BIOS

PRE-DEPLOYMENT



JAMI LaCHAPELLE
//PROJECT COORDINATOR

Jami has worked as a project coordinator since March 2015. In this role, she is responsible for scheduling on-site deployment activities and assigning Axon staff to each project.

Jami has been with Axon since May 2000. Prior to her current role, she was a training coordinator for four years, a training manager for three years, a research and development project coordinator for two years, and a technical services coordinator for six years.

DEPLOYMENT



CHRIS AERTS
//STRATEGIC DEPLOYMENT MANAGER

Chris has worked as a strategic deployment manager since November of 2021. In this role, he schedules on-site resources and oversees all aspects of the deployment process. He generally works with large agencies in the western U.S.

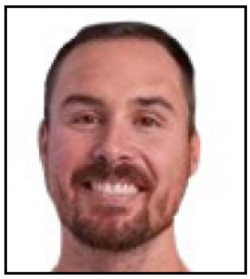
Chris formally worked as a customer support manager and project manager for Motorola Solutions.

Before joining Axon, Chris worked as a police officer with New Mexico State University for two years. He also worked as a firefighter, Lieutenant, and Captain for nine years with Doña Ana County, NM, and New Mexico State University Fire Departments.

Chris has worked on notable projects for:

- Riverside County Sheriff's Office, CA
- Metra Police Department, IL
- Travis County Sheriff's Office, TX
- Columbus Police Department, OH

He holds an A.A.S. from New Mexico State University.



MATT SCHLETER

//CUSTOMER SUCCESS MANAGER

Matt has worked at Axon as a customer success manager since January 2020. In this role, he works exclusively with agencies on the west coast of the United States to support their day-to-day needs and help them realize the most value from their investment with Axon. To do so, he provides education on new workflows and features, emerging technologies, and opportunities to enhance existing solutions. Additionally, as a customer success manager, Matt will to be the main point of contact for San Diego PD if any questions arise or if help is needed with your Axon solution.

Prior to joining Axon, Matt worked as a customer success manager for WebPT. Additionally, Matt was a military police officer in the U.S. Air Force for four years.

Matt's current clients include:

- Los Angeles Police Department, CA
- Los Angeles County Sheriff's Office, CA
- Las Vegas Metropolitan Police Department, NV

Matt holds a B.S. in Business Administration from the University of Arizona.

13. SECURITY AND PRIVACY

The successful Proposer (Awardee) shall at all times use its best efforts but in no event less than current industry best practices to protect the security and privacy of all City data where "security" is defined as protection of software and data from natural and human-caused hazards, and where "privacy" is defined as protection of software and data from unauthorized access and manipulation. Proposer shall also assure integrity of data by establishing and maintaining safeguards against the destruction, loss, or unauthorized alteration of City's data. Proposer shall, to the greatest extent possible, prevent security and privacy breaches, to address contingencies in the event of an unavoidable security or privacy breach, and to provide recovery and backup operation. Proposer shall comply with all security rules and regulations as it pertains to the San Diego Police Department and City of San Diego.

Axon will comply with all security rules and regulations as it pertains to the San Diego Police Department and City of San Diego.

ACCESS TO CLIENT DATA

All customer access to data is controlled at layer 7 of the OSI model within the web application interface over HTTPS. Additionally, Axon Evidence enables SDPD to control access at layer 4 of the OSI model by establishing IP whitelisting to define and limit the IP ranges in which a user may access Axon Evidence. Axon also protects Axon Evidence at layer 4 by blacklisting known malicious IP addresses. Axon protects and controls access on behalf of all Axon Evidence customers at layer 3 of the OSI model. Customer data is uniquely identified and marked to ensure appropriate segregation of customer data.

To protect the web application, Axon deploys a web application firewall (WAF) to actively protect against threats in real-time. Additionally, Axon performs frequent penetration testing of Axon Evidence. Penetration testing includes testing to ensure customer data segregation is maintained and not commingled.

ENCRYPTION

All evidence data is encrypted at rest and in transit. Robust SSL/TLS is implemented for data in transit using TLS 1.2 with a 256-bit connection and Perfect Forward Secrecy. Evidence data stored at rest is encrypted with at least 256-bit AES.

DISASTER RECOVERY AND CONTINUITY PLAN

Axon has designed Axon Evidence to be highly scalable and extremely resilient. Axon Evidence customer data is stored within data centers located in the continental United States. All data centers offer world-class security and system protection. All data centers employ backup power, climate control, alarms, and seismic bracing.

In the event of a major disaster that results in a full loss of a Microsoft Azure region, Axon has created the Axon Evidence Information System Contingency Plan (ISCP). The ISCP focuses on the recovery of Axon Evidence to a secondary Microsoft Azure region.

Axon is confident, that in the event of the complete destruction of a primary Microsoft Azure region, Axon Evidence can be recovered and restored in the secondary Microsoft Azure region within, at most, a 24-hour window. However, Axon views the likelihood of such an occurrence as negligible given the architecture of the underlying Microsoft Azure services.

The application's highly resilient architecture and application delivery is supported by the Service Level Agreement established with Axon's customer base.

Axon maintains a Business Continuity Plan that encompasses Axon Evidence operations and resiliency capabilities. This plan is reviewed periodically and is ISO 27001 certified.

SECURE DEVELOPMENT

Design, development, and maintenance of Axon Evidence are performed by Axon personnel within authorized facilities. These facilities are included in the scope of Axon's International Information Security Program. SDPD data stored within Axon Evidence will remain in the United States.

Axon has developed and operates secure software development lifecycle procedures (SDLC). Execution within the SDLC ensures security is evaluated at every phase of development and that quality measures are met. Axon does not outsource the development of Axon Evidence and development resources are assigned and dedicated to the on-going development, quality, and security of the product.

RISK DETECTION

Axon Evidence employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks.

Axon maintains a robust information security program designed to provide a high level of protection against current and emerging threats. This includes logging all access to evidence data and systems, and robust evidence audit reports within Axon Evidence.

The Axon Evidence infrastructure utilizes a multi-tier design that segregates the database tier from web and application tiers using firewalls and network ACLs. Axon Evidence utilizes host-based firewalls on all applicable systems. Host-based IDS and AV are deployed on applicable systems.

Criminal Justice Information Services (CJIS) Security Policy. Contractor acknowledges and shall comply with the requirements in U.S. Department of Justice, Federal Bureau of Investigation, (CJIS) Security Policy. A copy of (CJIS) Security Policy is attached as Attachment II to the Contract and is incorporated herein by reference.

Yes. Axon Evidence was designed and is operated to ensure that it is compliant with the FBI CJIS Security Policy. Customers can be assured that their digital data is protected by a robust information security program that is designed to exceed the CJIS security requirements as well as provide protection against current and emerging threats.

Axon acknowledges and abides by all aspects of the CJIS Security Addendum, and we are contractually committed to meeting CJIS, as the CJIS Security Addendum is included by reference into the Axon Master Services and Purchasing Agreement.

All Axon CJIS-authorized personnel are required to complete CJIS security training in compliance with the CJIS Security Policy. Axon uses 'CJIS Online' from Peak Performance Solutions to conduct and coordinate CJIS-specific security training. Axon personnel training records are available to customers within the CJIS Online System. Any additional SDPD-specific security awareness training can be conducted as required.

In addition to security awareness training, Axon CJIS-authorized personnel have undergone state and federal fingerprint-based checks in certain states. Axon is prepared to coordinate with SDPD to ensure that all Axon CJIS-authorized personnel undergo checks in alignment with the requirements of SDPD. Axon's CJIS compliance status has been validated independently by CJIS ACE and the underlying security program is audited on at least an annual basis by an additional third party as part of Axon's ISO 27001 program.

The Axon CJIS Compliance White paper (found here) outlines the specific security policies and practices for Axon Evidence and how they are compliant with the CJIS Security Policy.

SECURITY COMPLIANCE CERTIFICATIONS

Axon deploys a comprehensive Information Security Program (ISP) to ensure the confidentiality, integrity, and availability of all customer data in Axon Evidence. Security is integrated throughout Axon products, development processes, and corporate culture to ensure the security of data and maintain trust with customers.

ISO/IEC 27001:2013 CERTIFIED - INFORMATION SECURITY MANAGEMENT STANDARDS

The ISO/IEC 27001:2013 certificate validates that Axon has implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

ISO/IEC 27701:2019 CERTIFIED - CODE OF PRACTICE FOR PRIVACY INFORMATION MANAGEMENT

The ISO/IEC 27701:2019 certificate validates that Axon has implemented the internationally recognized control objectives, controls and guidelines related to implementing, maintaining, and continually improving a Privacy Information Management System (PIMS) in accordance with the privacy principles in ISO/IEC 29100 for a cloud computing environment.

ISO/IEC 27017:2015 CERTIFIED - CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

The ISO/IEC 27017:2015 certificate validates that Axon has implemented additional controls that enhance and refine those found in the ISO 27002 standard. ISO 27002 provides best practices and guidance for implementing the controls found in ISO 27001. ISO 27017 controls address cloud-specific concerns and detail the responsibilities of cloud service customers and cloud service providers, two categories into which Axon alternately falls depending on the specific control.

ISO/IEC 27018:2019 CERTIFIED - CODE OF PRACTICE FOR PROTECTING PERSONAL DATA IN THE CLOUD

The ISO/IEC 27018:2019 certificate validates that Axon has implemented the internationally recognized control objectives, controls, and guidelines related to the protection of Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for a cloud computing environment.

CALEA STANDARD 17.5.4 COMPLIANCE

Axon Evidence is aligned with the Commission on Accreditation for Law Enforcement Agencies (CALEA) standard related to Electronic Data Storage in the context of utilizing a service provider (17.5.4). Determining conformity with CALEA standards is a requirement for customers to make individually.

SOC 2+ AND SOC 3 REPORTS

Axon Cloud Services and the Axon AI Training Center have achieved AICPA SOC 2 Type 2 reporting. Axon's SOC 2 audit gauges the effectiveness of the services based on the AICPA Trust Service Principles and Criteria, as well as the Cloud Security Alliance Cloud Controls Matrix†, FBI Criminal Justice Information Services Security Policy, and the UK National Cyber Security Centre Cloud Security Principles†. The Axon SOC 2+ reports include a comprehensive description of the Axon Cloud Services and AI Training Center environments in addition to an assessment of the fairness of Axon's description of its controls. The SOC 2+ evaluates whether controls are designed appropriately, were in operation on a specified date, and were operating effectively over a specified time period. Axon is audited annually by independent third-party auditors against the SOC criteria and additional frameworks listed above.

For organizations who need assurance over the security, availability, and confidentiality of Axon Cloud Services, but do not need a detailed system description or comprehensive list of system controls, Axon also makes available a SOC 3 report. This report is provided by the third-party auditing firm and is intended as an summary of the audit engagement, and consists of the independent service auditor's report, an assertion of Axon management, brief system description, and an overview of the applicable service commitments selected for the audit. A copy of Axon's SOC 3 report can be found here.

† Criteria apply to Axon Cloud Services only.

Please note that sharing SOC+2 report results requires an executed non-disclosure agreement between Axon and SDPD.

CLOUD SECURITY ALLIANCE - CSA STAR ATTESTATION (LEVEL TWO)

Axon has been awarded CSA STAR Attestation. STAR Attestation consists of a rigorous third-party independent assessment of Axon Evidence against the CSA's Cloud Controls Matrix (CCM). Detailed results of the STAR Attestation testing are included in the Axon SOC 2+ report.

CLOUD SECURITY ALLIANCE - CSA STAR SELF-ASSESSMENT (LEVEL ONE)

Axon's Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) response provides detailed information about how Axon fulfills the security, privacy, compliance, and risk management requirements defined in the CCM and Consensus Assessments Initiative Questionnaire (CAIQ) version 3.0.1.

ACCESSIBILITY CONFORMANCE REPORT - WCAG 2.0 & VPAT/SECTION 508

Axon has created the Axon Evidence Accessibility Conformance Report for the purpose of assessing Axon Evidence compliance with the Web Content Accessibility Guidelines (WCAG) 2.0. The report covers the degree of conformance for WCAG 2.0 and U.S. Section 508 Standards.

FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP)

Axon has achieved a FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the High Impact Level. The authorization confirms that Axon Evidence has been reviewed and approved by the Departments of Defense and Homeland Security, and the General Services Administration. This enables the US Federal community to streamline their own authorization processes of Axon Evidence. Axon's FedRAMP authorization is for the US Federal Region of Axon Evidence. Learn more at axon.com/fedramp.

City IT Standards and Guidelines. Contractor acknowledges and shall comply with the requirements in City of San Diego IT Standards and Guideline. A copy of IT is attached as Attachment III to the Contract and is incorporated herein by reference.

Axon has reviewed and will comply with the requirements in City of San Diego IT Standards and Guideline, received with the bid documents.

14. SUBCONTRACTORS

Proposer shall not use Subcontractors to provide any labor, facilities, equipment, accessories, tools and other items and do any work required under the Scope of Work unless expressly agreed to by City in writing.

Not applicable. Subcontractors will not be used on this project.

15. DELIVERY

All deliverables described in this Scope of Work and training requirements must be completed within 30 days of execution of the contract. However, the City will consider and evaluate timelines submitted that exceed the 30-day timeline.

All deliveries under this contract shall be made to San Diego Police Department Headquarters located at:

San Diego Police Department – Operational Support

1401 Broadway

San Diego, CA 92101

All deliverables described in the Scope of Work and training requirements will be completed within 30 days of contract execution.

16. RETURNS

Returns of inoperable and/or damaged equipment will be returned to the successful Proposer at no cost to the City.

Yes. Axon will accept returns of inoperable and or/damaged equipment at no cost to the City.

17. REFERENCE CHECKS

REFERENCES

1. Company Name: Phoenix Police Department

   Contact Name and Phone Number: Geri Padilla, IT; 602-262-4913

   Contact Email: geri.padilla@phoenix.gov

   Address: 620 W Washington St, Phoenix, AZ 85003

   Contract Date: June 2023 – 5 Year

   Contract Amount: $35,501,131

   Requirements of Contract: Body-worn camera program combined with extensive bundle of Evidence.com features such as Performance, Redaction Assistant, Unlimited 3rd Party storage, and Unlimited Transcription. Deployment of 3,129 body worn cameras and licenses.

2. Company Name: Atlanta Police Department

   Contact Name and Phone Number: Sergeant Paul Bryant, 404-623-3201

   Contact Email: pabryant@atlantaga.gov

   Address: 226 Peachtree St SW Atlanta, GA 30303

   Contract Date: March 2023, 12 Year, Contract Amount: $105,673,922

   Requirements of Contract: Officer Safety Program, combined body-worn camera, Taser, deployment services, storage, licensing, Fleet (in-car cameras), Records (RMS), Interview, and AIR (UAV program) for 2,100 personnel.

3. Company Name: Santa Clara County Sheriff's Office

   Contact Name and Phone Number: Sergeant Ryan Dunn, 408-623-7518

   Contact Email: ryan.dunn@shf.sccgov.org

   Address: 55 West Younger Avenue San Jose, CA 95110

   Contract Date: December 2022, Contract Amount: $15,410,400.00

   Requirements of Contract: 2:1 Body Worn Camera Workflow, 1,275 body-worn cameras, deployment services, storage, and licensing. (Unlimited 7 Premium).

4. Company Name: Los Angeles Police Department

   Contact Name and Phone Number: Robert Bean, Sergeant II, Office: 213-486-0370, Mobile: 213-864-6417

   Contact Email: 37151@lapd.online

   Address: 100 West 1st Street, Suite 842, Los Angeles, CA 90012

   Contract Date: May 2020, Contract Amount: $52,000,000

   Requirements of Contract: 1,500 Fleet Vehicles, 7,255 body-worn cameras, Video Evidence Management, Warranty and Implementation Services

5. Company Name: Los Angeles Sheriff's Department

   Contact Name and Phone Number: Lieutenant Geoffrey Chadwick, Office: (562) 345-2730, Mobile: (213) 238-0751

   Contact Email: gnchadwi@lasd.org

   Address: 12440 Imperial Highway, Norwalk, CA 90650

   Contract Date: August 2020, Contract Amount: $25,610974.00

   Requirements of Contract: 5,248 Body Worn Cameras, Video Evidence Management, Warranty and Implementation Services.

City of San Diego

CONTRACTOR STANDARDS

Pledge of Compliance

The City of San Diego has adopted a Contractor Standards Ordinance (CSO) codified in section 22.3004 of the San Diego Municipal Code (SDMC). The City of San Diego uses the criteria set forth in the CSO to determine whether a contractor (bidder or proposer) has the capacity to fully perform the contract requirements and the business integrity to justify the award of public funds. This completed Pledge of Compliance signed under penalty of perjury must be submitted with each bid and proposal. If an informal solicitation process is used, the bidder must submit this completed Pledge of Compliance to the City prior to execution of the contract. All responses must be typewritten or printed in ink. If an explanation is requested or additional space is required, Contractors must provide responses on Attachment A to the Pledge of Compliance and sign each page. Failure to submit a signed and completed Pledge of Compliance may render a bid or proposal non-responsive. In the case of an informal solicitation or cooperative procurement, the contract will not be awarded unless a signed and completed Pledge of Compliance is submitted. A submitted Pledge of Compliance is a public record and information contained within will be available for public review except to the extent that such information is exempt from disclosure pursuant to applicable law.

By signing and submitting this form, the contractor is certifying, to the best of their knowledge, that the contractor and any of its Principals have not within a five (5) year period – preceding this offer, been convicted of or had a civil judgement rendered against them for commission of a fraud or a criminal offense in connection with obtaining, attempting to obtain or performing a public (Federal, State or local) contract or subcontract.

"Principal" means an officer, director, owner, partner or a person having primary management or supervisory responsibilities within the firm. The Contractor shall provide immediate written notice to the Procurement Contracting Officer handling the solicitation, at any time prior to award should they learn that this Representations and Certifications was inaccurate or incomplete.

This form contains 10 pages, additional information may be submitted as part of *Attachment A.*

A. BID/PROPOSAL/SOLICITATION TITLE:

RFP Number: No. 10090080-24-E

BODY WORN CAMERA (BWC) SYSTEM

B. BIDDER/PROPOSER INFORMATION:

Axon Enterprise, Inc.			
Legal Name		DBA	
17800 N. 85th Street	Scottsdale	AZ	85255
Street Address	City	State	Zip
Megan Hardisty	(480) 253-7854	(480) 991-0791	
Contact Person, Title	Phone	Fax	

Provide the name, identity, and precise nature of the interest* of all persons who are directly or indirectly involved** in this proposed transaction (SDMC § 21.0103). Use additional pages if necessary.

* The precise nature of the interest includes:

- the percentage ownership interest in a party to the transaction,
- the percentage ownership interest in any firm, corporation, or partnership that will receive funds from the transaction,
- the value of any financial interest in the transaction,
- any contingent interest in the transaction and the value of such interest should the contingency be satisfied, and
- any philanthropic, scientific, artistic, or property interest in the transaction.

** Directly or indirectly involved means pursuing the transaction by:

- communicating or negotiating with City officers or employees,
- submitting or preparing applications, bids, proposals or other documents for purposes of contracting with the City, or
- directing or supervising the actions of persons engaged in the above activity.

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

Name | Title/Position

City and State of Residence | Employer (if different than Bidder/Proposer)

Interest in the transaction

Name | Title/Position

City and State of Residence | Employer (if different than Bidder/Proposer)

Interest in the transaction

Name | Title/Position

City and State of Residence | Employer (if different than Bidder/Proposer)

Interest in the transaction

C. OWNERSHIP AND NAME CHANGES:

1. In the past five (5) years, has your firm changed its name?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to list all prior legal and DBA names, addresses, and dates each firm name was used. Explain the specific reasons for each name change.

2. Is your firm a non-profit?
   ☐ **Yes** ☑ **No**

   If **Yes,** attach proof of status to this submission.

3. In the past five (5) years, has a firm owner, partner, or officer operated a similar business?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to list names and addresses of all businesses and the person who operated the business. Include information about a similar business only if an owner, partner, or officer of your firm holds or has held a similar position in another firm.

D. BUSINESS ORGANIZATION/STRUCTURE:

Indicate the organizational structure of your firm. Fill in only one section on this page. Use Attachment A if more space is required.

☐ **Corporation** Date incorporated: 04/05/2017 State of incorporation: Delaware

List corporation's current officers: President: Rick Smith, CEO
Vice Pres: _____
Secretary: _____
Treasurer: _____

Type of corporation: C ☑ Subchapter S ☐

Is the corporation authorized to do business in California: ☑ **Yes** ☐ **No**

If **Yes,** after what date: 06/22/2017

Is your firm a publicly traded corporation? ☑ **Yes** ☐ **No**

If **Yes,** how and where is the stock traded? NASDAQ

If **Yes**, list the name, title and address of those who own ten percent (10 %) or more of the corporation's stocks:

BlackRock, Inc. is currently the company's largest shareholder with 11% of shares outstanding.

Blackrock Inc.55 East 52nd Street New York, NY, USA 10055

Do the President, Vice President, Secretary and/or Treasurer of your corporation have a third party interest or other financial interests in a business/enterprise that performs similar work, services or provides similar goods? ☐ **Yes** ☑ **No**

If **Yes,** please use Attachment A to disclose.

Please list the following:	Authorized	Issued	Outstanding
a. Number of voting shares:			
b. Number of nonvoting shares:			
c. Number of shareholders:			
d. Value per share of common stock:		Par	$
		Book	$
		Market	$

Limited Liability Company Date formed: _____ State of formation: _____

List the name, title and address of members who own ten percent (10%) or more of the company:

☐ **Partnership** Date formed: _____ State of formation: _____

List names of all firm partners:

☐ **Sole Proprietorship** Date started: _____

List all firms you have been an owner, partner or officer with during the past five (5) years. Do not include ownership of stock in a publicly traded company:

☐ **Joint Venture** Date formed: _____

List each firm in the joint venture and its percentage of ownership:

Note: To be responsive, each member of a Joint Venture or Partnership must complete a separate *Contractor Standards form.*

E. FINANCIAL RESOURCES AND RESPONSIBILITY:

1. Is your firm preparing to be sold, in the process of being sold, or in negotiations to be sold?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain the circumstances, including the buyer's name and principal contact information.

2. In the past five (5) years, has your firm been denied bonding?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances; include bonding company name.

3. In the past five (5) years, has a bonding company made any payments to satisfy claims made against a bond issued on your firm's behalf or a firm where you were the principal?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

4. In the past five (5) years, has any insurance carrier, for any form of insurance, refused to renew the insurance policy for your firm?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

5. Within the last five years, has your firm filed a voluntary petition in bankruptcy, been adjudicated bankrupt, or made a general assignment for the benefit of creditors?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

6. Are there any claims, liens or judgements that are outstanding against your firm?
   ☑ **Yes** ☐ **No**

   If **Yes,** please use Attachment A to provide detailed information on the action.

7. Please provide the name of your principal financial institution for financial reference. By submitting a response to this Solicitation Contractor authorizes a release of credit information for verification of financial responsibility.

   Name of Bank: Chase

   Point of Contact: Dorian Andritoiu

   Address: 8501 N Scottsdale Rd, Ste 240, Scottsdale, AZ 85253

   Phone Number: (602) 221-2295

8. By submitting a response to a City solicitation, Contractor certifies that he or she has sufficient operating capital and/or financial reserves to properly fund the requirements identified in the solicitation. At City's request, Contractor will promptly provide to City

a copy of Contractor's most recent balance sheet and/or other necessary financial statements to substantiate financial ability to perform.

9. In order to do business in the City of San Diego, a current Business Tax Certificate is required. Business Tax Certificates are issued by the City Treasurer's Office. If you do not have one at the time of submission, one must be obtained prior to award.

   Business Tax Certificate No.: B2020005936 Year Issued: 2023

F. PERFORMANCE HISTORY:

1. In the past five (5) years, has your firm been found civilly liable, either in a court of law or pursuant to the terms of a settlement agreement, for defaulting or breaching a contract with a government agency?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

2. In the past five (5) years, has a public entity terminated your firm's contract for cause prior to contract completion?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances and provide principal contact information.

3. In the past five (5) years, has your firm entered into any settlement agreement for any lawsuit that alleged contract default, breach of contract, or fraud with or against a public entity?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

4. Is your firm currently involved in any lawsuit with a government agency in which it is alleged that your firm has defaulted on a contract, breached a contract, or committed fraud?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

5. In the past five (5) years, has your firm, or any firm with which any of your firm's owners, partners, or officers is or was associated, been debarred, disqualified, removed, or otherwise prevented from bidding on or completing any government or public agency contract for any reason?
   ☐ **Yes** ☑ **No**

   If **Yes**, use *Attachment A* to explain specific circumstances.

6. In the past five (5) years, has your firm received a notice to cure or a notice of default on a contract with any public agency?

   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances and how the matter resolved.

7. Performance References:

Please provide a minimum of three (3) references familiar with work performed by your firm which was of a similar size and nature to the subject solicitation within the last five (5) years.

Please note that any references required as part of your bid/proposal submittal are in addition to those references required as part of this form.

Company Name: Phoenix Police Department

Contact Name and Phone Number: Geri Padilla, IT; 602-262-4913

Contact Email: geri.padilla@phoenix.gov

Address: 620 W Washington St, Phoenix, AZ 85003

Contract Date: June 1, 2023

Contract Amount: $ 35,501,131.00

Requirements of Contract: Body-worn camera program combined with extensive bundle of Evidence.com features such as Performance, Redaction Assistant, Unlimited 3rd Party storage, and Unlimited Trans

Company Name: Atlanta Police Department

Contact Name and Phone Number: Sergeant Paul Bryant, 404-623-3201

Contact Email: pabryant@atlantaga.gov

Address: 226 Peachtree St SW Atlanta, GA 30303

Contract Date: March 1, 2023

Contract Amount: $ 105,673,922.00

Requirements of Contract: Officer Safety Program, combined body-worn camera, Taser, deployment services, storage, licensing, Fleet (in-car cameras), Records (RMS), Interview, and AIR (UAV program) for

Company Name: Santa Clara County Sheriff's Office

Contact Name and Phone Number: Sergeant Ryan Dunn, 408-623-

Contact Email: ryan.dunn@shf.sccgov.org

Address: 55 West Younger Avenue San Jose, CA 95110

Contract Date: December 1, 2022

Contract Amount: $ 15,410,400.00

Requirements of Contract: 2:1 Body Worn Camera Workflow, 1,275 body-worn cameras, deployment services, storage, and licensing. (Unlimited 7 Premium).

G. COMPLIANCE:

1. In the past five (5) years, has your firm or any firm owner, partner, officer, executive, or manager been criminally penalized or found civilly liable, either in a court of law or pursuant to the terms of a settlement agreement, for violating any federal, state, or local law in performance of a contract, including but not limited to, laws regarding health and safety, labor and employment, permitting, and licensing laws?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances surrounding each instance. Include the name of the entity involved, the specific infraction(s) or violation(s), dates of instances, and outcome with current status.

2. In the past five (5) years, has your firm been determined to be non-responsible by a public entity?
   ☐ **Yes** ☑ **No**

If **Yes**, use Attachment A to explain specific circumstances of each instance. Include the name of the entity involved, the specific infraction, dates, and outcome.

H. BUSINESS INTEGRITY:

1. In the past five (5) years, has your firm been convicted of or found liable in a civil suit for making a false claim or material misrepresentation to a private or public entity?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance. Include the entity involved, specific violation(s), dates, outcome and current status.

2. In the past five (5) years, has your firm or any of its executives, management personnel, or owners been convicted of a crime, including misdemeanors, or been found liable in a civil suit involving the bidding, awarding, or performance of a government contract?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance; include the entity involved, specific infraction(s), dates, outcome and current status.

3. In the past five (5) years, has your firm or any of its executives, management personnel, or owners been convicted of a federal, state, or local crime of fraud, theft, or any other act of dishonesty?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance; include the entity involved, specific infraction(s), dates, outcome and current status.

4. Do any of the Principals of your firm have relatives that are either currently employed by the City or were employed by the City in the past five (5) years?

   ☐**Yes** ☑**No**

   If **Yes,** please disclose the names of those relatives in Attachment A.

I. BUSINESS REPRESENTATION:

1. Are you a local business with a physical address within the County of San Diego?
☐**Yes** ☑**No**

2. Are you a certified Small and Local Business Enterprise certified by the City of San Diego?
☐**Yes** ☑**No**

   Certification #_____

3. Are you certified as any of the following:
   a. Disabled Veteran Business Enterprise Certification #_____
   b. Woman or Minority Owned Business Enterprise Certification # _____
   c. Disadvantaged Business Enterprise Certification #_____

J. WAGE COMPLIANCE:

In the past five (5)years, has your firm been required to pay back wages or penalties for failure to comply with the federal, state or local **prevailing, minimum, or living wage laws?** ☐**Yes** ☑**No** If **Yes**, use Attachment A to explain the specific circumstances of each instance. Include the entity involved, the specific infraction(s), dates, outcome, and current status.

By signing this Pledge of Compliance, your firm is certifying to the City that you will comply with the requirements of the Equal Pay Ordinance set forth in SDMC sections 22.4801 through 22.4809.

K. STATEMENT OF SUBCONTRACTORS & SUPPLIERS:

Please provide the names and information for all subcontractors and suppliers used in the performance of the proposed contract, and what portion of work will be assigned to each subcontractor. Subcontractors may not be substituted without the written consent of the City. Use Attachment A if additional pages are necessary. If no subcontractors or suppliers will be used, please write "Not Applicable."

Company Name: _____

Address: _____

Contact Name: _____ Phone: _____ Email: _____

Contractor License No.: _____ DIR Registration No.: _____

Sub-Contract Dollar Amount: $_____ (per year) $_____ (total contract term)

Scope of work subcontractor will perform: _____

Identify whether company is a subcontractor or supplier: _____

Certification type (check all that apply):☐DBE ☐DVBE ☐ELBE ☐MBE ☐SLBE☐WBE ☐Not Certified

Contractor must provide valid proof of certification with the response to the bid or proposal to receive participation credit.

Company Name: _____

Address: _____

Contact Name: _____ Phone: _____ Email: _____

Contractor License No.: _____ DIR Registration No.: _____

Sub-Contract Dollar Amount: $_____ (per year) $_____ (total contract term)

Scope of work subcontractor will perform: _____

Identify whether company is a subcontractor or supplier: _____

Certification type (check all that apply):☐DBE ☐DVBE ☐ELBE ☐MBE ☐SLBE☐WBE ☐Not Certified

Contractor must provide valid proof of certification with the response to the bid or proposal to receive participation credit.

L. STATEMENT OF AVAILABLE EQUIPMENT:

A full inventoried list of all necessary equipment to complete the work specified may be a requirement of the bid/proposal submission.

By signing and submitting this form, the Contractor certifies that all required equipment included in this bid or proposal will be made available one week (7 days) before work shall commence. In instances where the required equipment is not owned by the Contractor, Contractor shall explain how the equipment will be made available before the commencement of work. The City of San

Diego reserves the right to reject any response, in its opinion, if the Contractor has not demonstrated he or she will be properly equipped to perform the work in an efficient, effective matter for the duration of the contract period.

M. TYPE OF SUBMISSION: This document is submitted as:

☑ Initial submission of *Contractor Standards Pledge of Compliance*

☐ Initial submission of *Contractor Standards Pledge of Compliance* as part of a Cooperative agreement

☐ Initial submission of *Contractor Standards Pledge of Compliance* as part of a Sole Source agreement

☐ Update of prior *Contractor Standards Pledge of Compliance* dated _____.

Complete all questions and sign below.

Under penalty of perjury under the laws of the State of California, I certify that I have read and understand the questions contained in this Pledge of Compliance, that I am responsible for completeness and accuracy of the responses contained herein, and that all information provided is true, full and complete to the best of my knowledge and belief. I agree to provide written notice to the Purchasing Agent within five (5) business days if, at any time, I learn that any portion of this Pledge of Compliance is inaccurate. Failure to timely provide the Purchasing Agent with written notice is grounds for Contract termination.

I, on behalf of the firm, further certify that I and my firm will comply with the following provisions of SDMC section 22.3004:

(a) I and my firm will comply with all applicable local, State and Federal laws, including health and safety, labor and employment, and licensing laws that affect the employees, worksite or performance of the contract.

(b) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of receiving notice that a government agency has begun an investigation of me or my firm that may result in a finding that I or my firm is or was not in compliance with laws stated in paragraph (a).

(c) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of a finding by a government agency or court of competent jurisdiction of a violation by the Contractor of laws stated in paragraph (a).

(d) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of becoming aware of an investigation or finding by a government agency or court of competent jurisdiction of a violation by a subcontractor of laws stated in paragraph (a).

(e) I and my firm will cooperate fully with the City during any investigation and to respond to a request for information within ten (10) working days.

Failure to sign and submit this form with the bid/proposal shall make the bid/proposal non-responsive. In the case of an informal solicitation, the contract will not be awarded unless a signed and completed *Pledge of Compliance* is submitted.

Robert Driscoll, VP, Associate General Counsel and Assistant Corporate Secretary		08/15/2023
Name and Title	Signature	Date

City of San Diego
CONTRACTOR STANDARDS
Attachment "A"

Provide additional information in space below. Use additional Attachment "A" pages as needed. Each page must be signed. Print in ink or type responses and indicate question being answered.

I have read the matters and statements made in this Contractor Standards Pledge of Compliance and attachments thereto and I know the same to be true of my own knowledge, except as to those matters stated upon information or belief and as to such matters, I believe the same to be true. I certify under penalty of perjury that the foregoing is true and correct.

Robert Driscoll, VP, Associate General Counsel and Assistant Corporate Secretary		08/15/2023
Print Name, Title	Signature	Date