Axon Cloud Services CJIS Compliance Guide

Table of Contents

Executive Summary

The Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy sets the minimum-security requirements to provide an acceptable level of assurance to protect the full lifecycle of Criminal Justice Information (CJI). Agencies using cloud-based services are required to make informed decisions on whether the cloud provider can offer services that maintain compliance with the requirements of the CJIS Security Policy.

Adopting a cloud-based platform, such as Axon Cloud Services, allows a transference of responsibility from your agency to the provider. Additional benefits of Axon Cloud Services include:

- Designed and operated to ensure compliance to CJIS Security Policy.
- Staff members with access or exposure to unencrypted CJI trained and vetted IAW CJIS Personnel Security controls.
- Aligned to CALEA Standards related to Electronic Data Storage.
- Assessed annually against the AICPA SOC2 Type 2 Trust Principles with integrated CJIS Security Policy v5.9.1 control validation. The report is available upon request by contacting your sales representative or at infosec@axon.com.
- Integrated service continuity and disaster recovery and resiliency capabilities with testing. A customer overview of Axon's Business Continuity Plan is available upon request by contacting your sales representative or at infosec@axon.com.
- To date, free of breaches and unauthorized leaks or disclosures of customer data while maintaining Cyber Risk Insurance Policy (available in **Attachment A: Certificate of Liability Insurance** of this document).
- Axon operates the only Digital Evidence Management platform with a FedRAMP (High) Joint Authorization Board Provisional Authority to Operate for our Federal customers; Axon Cloud Services is committed to leading the way with StateRAMP requirements for our State, Local, Tribal and Territorial customers.

This document outlines the specific security policies and practices for Axon Cloud Services and how they are compliant with the CJIS Security Policy, version 5.9.1. Axon has leveraged CJIS's Requirements Companion Document to provide details on control responsibilities when agencies use Axon Cloud Services. The Requirements Companion Document is provided as an additional resource within the CJIS Security Policy Resource Center and describes which party has responsibility to perform the actions necessary to ensure a particular CJIS Security Policy requirement is being met.

Attachment E: CJIS Appendix G.3 Cloud Computing of this document provides responses to questions posed in the CJIS Security Policy Appendix G.3 Cloud Computing at the end of this document.

Additional detail regarding Axon's CJIS commitment is detailed https://www.axon.com/cjis-security-policy-compliance.

You can always find the latest on Axon's compliance and security programs at https://www.axon.com/trust/compliance and https://www.axon.com/trust

Purpose

This document serves as a guide for customers of Axon solutions in ensuring they meet or exceed the security control requirements outlined in CJIS Security Policy 5.9.1. Based on the Axon Master Services and Purchasing Agreement, roles and responsibilities between Axon and its customer are delineated.

This guide also updates the CJIS control mappings for CJIS Security Policy version 5.9.1 and NIST 800-53 version 5. For an overview, see **Attachment F1: Control Crosswalk NIST 800-53v5 to CJIS 5.9.1**.

This guide can also aid in your agency building out a holistic Information Security & Privacy program by integrating CJIS requirements into the NIST CSF. For an overview, see **Attachment F2: Control Crosswalk NIST CSF v1.1 to CJIS 5.9.1**.

How to Use This Guide

In the chapters below, Axon has broken out each CJIS 5.9.1 security control by policy area. These controls have been validated by an independent third-party assessor as part of the annual Axon Cloud Services SOC2 report. Within each chapter, the individual security controls have been placed into a box. Each box contains the following sections:

- Section 1: CJIS Control Number and Name
- Section 2: Control Statement
- Section 3: Control Guidance
- Section 4: Control Mappings
- Section 5: SOC Report
- Section 6: Agency Responsibility
- Section 7: Axon Responsibility
- Section 8: Implementation Support

CJIS Control Number and Name	
Control Statement	Narrative of the CJIS Security Policy Control.
Control Owner	Who owns responsibility of the control: Agency/Axon/Shared/3rd Party.
Mapping	This section identifies mappings to Information Security frameworks to aid in understanding how the CJIS control integrates into an overall ISMS. Crosswalks of CJIS 5.9.1 to NIST 800-53v5 and NIST CSF can be found in **Attachment E: Crosswalks**.
SOC Report	This section identifies the corresponding control within the Axon Cloud Services SOC2 report validating efficacy of the CJIS Policy v5.9.1 control.
Agency Responsibility	This section will outline the responsibilities of the Axon customer in implementing the control.
Axon Responsibility	This section will outline the responsibilities of Axon in implementing the control.
Implementation Support	This section will identify NIST resources mapped to the NIST 800-53v5 controls for implementing the control(s).
Related Controls	Identifies relationships and dependencies to the listed control.

Additional support can be requested by your Axon Sales representative or contacting InfoSec@axon.com.

CJIS Security Policy Area 1 – Information Exchange Agreements

5.1.1 Information Exchange	
Control Statement	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.
Control Owner	Agency
Mapping	**CSF**: ID.SC-3 **NIST**: AC-21, CA-3, SA-2, SA-4, SA-4(1), SR-6
SOC Report	Out of Scope
Agency Responsibility	Agencies are responsible for establishing information exchange agreements with parties with whom they share data through Axon Cloud Services. Appendix D of the CJIS Security Policy provides additional guidance and examples to meet this control.
Axon Responsibility	Axon's contractual agreement with the agency outlines the data protection roles, responsibilities, and data ownership.
Implementation Guidance	**AC-21**: NIST 800-150; NISTIR 8062 **CA-3**: FIPS 199; NIST 800-47 **SA-4**: FIPS-140-2; FIPS 201; NIST 800-23; NIST 800-35; NIST 800-36; NIST 800-37; NIST 800-64; NIST 800-70; NIST 800-73; NIST 800-137; NIST-800-161; NISTIR 7539; NISTIR 7622; NISTIR 7676; NISTIR 7870; NISTIR 8062 **SR-6**: NIST 800-30; NIST 800-161; NISTIR 7622; NISTIR 8272

5.1.1.1 Information Handling	
Control Statement	Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse.
Control Owner	Agency
Mapping	**CSF**: ID.SC-3 **NIST**: AC-21, CM-9, CP-6, CP-7, IR-8, PL-2, PM-1
SOC Report	Out of Scope
Agency Responsibility	Agencies must establish policies related to the access and usage of data stored within Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices within Axon Cloud Services for securely handling information. The Axon contract for services and MSPA establishes an Information Exchange Agreement between itself and the agency.
Implementation Guidance	**AC-21**: NIST 800-150; NISTIR 8062 **CM-9**: NIST 800-128 **CP-6**: NIST 800-34 **CP-7**: NIST 800-34 **IR-8**: NIST 800-61 **PL-2**: NIST 800-18 **PM-1**: NIST 800-37; NIST 800-39

5.1.1.2 State and Federal Agency User Agreements	
Control Statement	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 per authorization of Department of Justice (DOJ) Order 2640.2F. All user agreements with the FBI CJIS Division **shall** be coordinated with the CSA head.
Control Owner	Agency
Mapping	**CSF**: ID.SC-3 **NIST**: AC-21, CA-3, SA-2, SA-4, SA-4(1), SR-6
SOC Report	Out of Scope
Agency Responsibility	CSA heads or SIB Chiefs are responsible for maintaining this written agreement. CSA heads or SIB Chiefs are responsible for maintaining this written agreement. CSA heads or SIB Chiefs are responsible for maintaining this written agreement. CSA heads or SIB Chiefs are responsible for maintaining this written agreement.
Axon Responsibility	N/A; Axon has no role or responsibilities with this security control. CSA heads or SIB Chiefs are responsible for maintaining this written agreement.
Implementation Guidance	**AC-21**: NIST 800-150; NISTIR 8062 **CA-3**: FIPS 199; NIST 800-47 **SA-2**: NIST 800-65 **SA-4**: FIPS-140-2; FIPS 201; NIST 800-23; NIST 800-35; NIST 800-36; NIST 800-37; NIST 800-64; NIST 800-70; NIST 800-73; NIST 800-137; NIST-800-161; NISTIR 7539; NISTIR 7622; NISTIR 7676; NISTIR 7870; NISTIR 8062 **SR-6**: NIST 800-30; NIST 800-161; NISTIR 7622; NISTIR 8272

5.1.1.3 Criminal Justice Agency User Agreements	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: ID.SC-3 **NIST**: AC-21, CA-3, SA-2, SA-4, SA-4(1), SR-6
SOC Report	Out of Scope
Agency Responsibility	The State CSA and agency LASO are responsible for maintaining this written agreement. Appendix D.1 CJIS User Agreement of the CJIS Security Policy provides additional guidance and examples to meet this control.
Axon Responsibility	N/A; Axon has no role or responsibilities with this security control.
Implementation Guidance	**AC-21**: NIST 800-150; NISTIR 8062 **CA-3**: FIPS 199; NIST 800-47 **SA-2**: NIST 800-65 **SA-4**: FIPS-140-2; FIPS 201; NIST 800-23; NIST 800-35; NIST 800-36; NIST 800-37; NIST 800-64; NIST 800-70; NIST 800-73; NIST 800-137; NIST-800-161; NISTIR 7539; NISTIR 7622; NISTIR 7676; NISTIR 7870; NISTIR 8062 **SR-6**: NIST 800-30; NIST 800-161; NISTIR 7622; NISTIR 8272

5.1.1.4 Interagency and Management Control Agreements	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: ID.SC-3 **NIST**: AC-21, CA-3, SA-2, SA-4, SA-4(1), SR-6
SOC Report	Out of Scope
Agency Responsibility	The agency LASO and appropriate NCJA representative are responsible for maintaining this written agreement. Appendixes D.2 Management Control Agreement and D.4 Interagency Connection Agreement of the CJIS Security Policy v5.9 provides additional guidance and examples to meet this control.
Axon Responsibility	N/A; Axon has no role or responsibilities with this security control.
Implementation Guidance	**AC-21**: NIST 800-150; NISTIR 8062 **CA-3**: FIPS 199; NIST 800-47 **SA-2**: NIST 800-65 **SA-4**: FIPS-140-2; FIPS 201; NIST 800-23; NIST 800-35; NIST 800-36; NIST 800-37; NIST 800-64; NIST 800-70; NIST 800-73; NIST 800-137; NIST-800-161; NISTIR 7539; NISTIR 7622; NISTIR 7676; NISTIR 7870; NISTIR 8062 **SR-6**: NIST 800-30; NIST 800-161; NISTIR 7622; NISTIR 8272

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum	
Control Statement	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. 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). 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).
Control Owner	Shared
Mapping	**CSF**: ID.AM-6 **NIST**: AC-21, CA-3, SA-2, SA-4, SA-4(1), SR-6
SOC Report	CJI-5.1.1.5-01
Agency Responsibility	Agencies are responsible for maintaining valid CJIS Security Addendums of Axon personnel. These addendums are an auditable artifact.
Axon Responsibility	Axon is responsible for ensuring valid CJIS Security Addendums for all personnel with access or exposure to unencrypted CJI and CHRI are provided to agencies. Addendums may be accessed through the CJISOnline portal or provided upon request.
Implementation Guidance	**AC-21**: NIST 800-150; NISTIR 8062 **CA-3**: FIPS 199; NIST 800-47 **SA-2**: NIST 800-65 **SA-4**: FIPS-140-2; FIPS 201; NIST 800-23; NIST 800-35; NIST 800-36; NIST 800-37; NIST 800-64; NIST 800-70; NIST 800-73; NIST 800-137; NIST-800-161; NISTIR 7539; NISTIR 7622; NISTIR 7676; NISTIR 7870; NISTIR 8062 **SR-6**: NIST 800-30; NIST 800-161; NISTIR 7622; NISTIR 8272

5.1.1.6 Agency User Agreements	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: ID.SC-2 **NIST**: AC-21, CA-3, SA-2, SA-4, SA-4(1), SR-6
SOC Report	Out of Scope
Agency Responsibility	Agencies are responsible for reviewing fingerprint-based background checks and adjudicating results of Axon personnel to determine suitability for access or exposure to agency unencrypted CJI.
Axon Responsibility	Axon maintains policies and procedures identifying roles and responsibilities which require access or exposure to unencrypted CJI and are approved for vetting by their respective Business Unit Manager. These personnel undergo nationwide fingerprint-based background checks through the state CSA, who provide adjudication results to both the agency and Axon.
Implementation Guidance	**AC-21**: NIST 800-150; NISTIR 8062 **CA-3**: FIPS 199; NIST 800-47 **SA-2**: NIST 800-65 **SA-4**: FIPS-140-2; FIPS 201; NIST 800-23; NIST 800-35; NIST 800-36; NIST 800-37; NIST 800-64; NIST 800-70; NIST 800-73; NIST 800-137; NIST-800-161; NISTIR 7539; NISTIR 7622; NISTIR 7676; NISTIR 7870; NISTIR 8062 **SR-6**: NIST 800-30; NIST 800-161; NISTIR 7622; NISTIR 8272

5.1.2 Monitoring, Review, and Delivery of Services	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: ID.SC-4 **NIST**: RA-3, SA-9, SA-9(1)
SOC Report	Out of Scope
Agency Responsibility	Agencies will submit requests for validation of security controls and adherence to requirements established under the Axon contract and MSPA.
Axon Responsibility	Axon will support agency requests for metrics and benchmarks, provide annual attestation reports, such as SOC2, upon request.
Implementation Guidance	**RA-3**: NIST 800-30; NIST 800-39; NIST 800-161; NISTIR 8023 **SA-9**: NIST 800-35; NIST 800-161

5.1.2.1 Managing Changes to Service Providers	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: ID.SC-1 **NIST**: RA-3
SOC Report	Out of Scope
Agency Responsibility	Agencies are responsible for assessing the risks involved incorporating new vendors and services through an established Supply Chain Risk Management Program.
Axon Responsibility	Coordination of service changes will be managed by Professional Services and Customer Success. Axon will assist in agency completion of risk assessments and Business Impact Analysis.
Implementation Guidance	**RA-3**: NIST 800-30; NIST 800-39; NIST 800-161; NISTIR 8023

5.1.3 Secondary Dissemination	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: ID.AM-3 **NIST**: PS-3, PS-6, PS-7
SOC Report	Out of Scope
Agency Responsibility	Agencies are responsible for accounting for secondary dissemination of CHRI originating from their control.
Axon Responsibility	Third Party Service providers are accounted for in SOC2 report. Axon vendors undergo a risk assessment as part of a Supply Chain Risk Management program prior to onboarding and annually. Vendor Sub-processors are not permitted access or exposure to unencrypted CJI.
Implementation Guidance	**PS-3**: FIPS 199; FIPS 201; NIST 800-60-1; NIST 800-60-2; NIST 800-73-4; NIST 800-76-2; NIST 800-78-4 **PS-6**: NA **PS-7**: NIST 800-35; NIST 800-63-3

5.1.4 Secondary Dissemination of Non-CHRI CJI	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: ID.AM-3 **NIST**: PS-3, PS-6, PS-7
SOC Report	Out of Scope
Agency Responsibility	Agencies are responsible for accounting for secondary dissemination of Non-CHRI originating from their control.
Axon Responsibility	N/A
Implementation Guidance	**PS-3**: FIPS 199; FIPS 201; NIST 800-60-1; NIST 800-60-2; NIST 800-73-4; NIST 800-76-2; NIST 800-78-4 **PS-6**: NA **PS-7**: NIST 800-35; NIST 800-63-3

CJIS Security Policy Area 2 – Security Awareness Training

5.2 Basic Security Awareness Training	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AT-1 **NIST**: AT-1, PL-4, PL-4(1)
SOC Report	GRM-03-01; CJI-5.2.1-01
Agency Responsibility	Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.
Axon Responsibility	Axon maintains a comprehensive security awareness program which includes annual training. Authorized Axon personnel with access or exposure to unencrypted CJI are required to complete Level 4 CJIS Security Training upon assignment and biennially thereafter.
Implementation Support	**AT-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-50; NIST 800-100 **PL-4**: NIST 800-18

5.2.1.1 Level One Security Awareness Training	
Control Statement	At a minimum, the following topics **shall** be addressed as baseline security awareness training for all personnel who have 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.
Control Owner	Shared
Mapping	**CSF**: PR.AT-1; PR.AT-5 **NIST**: AT-2, AT-3
SOC Report	CJI-5.2.1-01
Agency Responsibility	Agencies are responsible for ensuring personnel undergo appropriate security awareness training before permitting access to physically secure locations maintained by the agency.
Axon Responsibility	Axon ensures personnel understand local protocols before permitting access to physically secure locations maintained on Axon campuses.
Implementation Support	**AT-2**: NIST 800-50 **AT-3**: NIST 800-50

5.2.1.2 Level Two Security Awareness Training	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AT-1; PR.AT-2; PR.AT-5 **NIST**: AT-2(2), AT-3, PL-4, PL-4(1)
SOC Report	CJI-5.2.1-01
Agency Responsibility	Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.
Axon Responsibility	Axon provides security awareness training to all employees which aligns to the requirements established under this control.
Implementation Support	**AT-2**: NIST 800-50 **AT-3**: NIST 800-50 **PL-4**: NIST 800-18

5.2.1.3 Level Three Security Awareness Training	
Control Statement	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 (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems. 16. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems. 17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.
Control Owner	Shared
Mapping	**CSF**: PR.AT-1; PR.AT-2; PR.AT-5 **NIST**: AT-2(2), AT-3, PL-4, PL-4(1)
SOC Report	CJI-5.2.1-01
Agency Responsibility	Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.
Axon Responsibility	Axon provides security awareness training to all employees which aligns to the requirements established under this control.
Implementation Support	**AT-2**: NIST 800-50 **AT-3**: NIST 800-50 **PL-4**: NIST 800-18

5.2.1.4 Level Four Security Awareness Training	
Control Statement	In addition to 5.2.1.1, 5.2.1.2 and 5.2.1.3 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.
Control Owner	Shared
Mapping	**CSF**: PR.AT-2; PR-AT-3 **NIST**: AT-3, CM-10
SOC Report	CJI-5.2.1-01
Agency Responsibility	Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.
Axon Responsibility	Axon maintains a comprehensive security awareness program. Training is provided for all employees and is required at least annually and within six months of employment. In addition to annual training, employees supporting Axon Cloud Services are required to complete CJIS Online training at Level 4 biennially.
Implementation Support	**AT-3**: NIST 800-50 **CM-10**: N/A

5.2.3 Security Training Records	
Control Statement	Records of individual basic security awareness training and specific information system security training **shall** be: • documented • kept current • maintained by the CSO/SIB/Compact Officer
Control Owner	Shared
Mapping	**CSF**: PR.IP-11 **NIST**: AT-4, PL-4
SOC Report	CJI-5.2.3-01
Agency Responsibility	Agencies are responsible for maintaining records of security awareness training for personnel who access Axon Cloud Services.
Axon Responsibility	Axon maintains a comprehensive security awareness program. Training is provided for all employees and is required at least annually and within six months of employment. In addition to annual training, employees supporting Axon Cloud Services are required to complete CJIS Online training at Level 4 biennially. Records of training can be provided to customers upon request or by accessing Axon's CJISOnline portal.
Implementation Support	**AT-4**: N/A **PL-4**: NIST 800-18

CJIS Security Policy Area 3 - Incident Response

5.3 Incident Response	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.IP-9 **NIST**: IR-1
SOC Report	SEF-01-01
Agency Responsibility	Agencies are responsible for establishing incident response capabilities and must report to Axon if they believe an unauthorized third party may be using their account or their content, or if their account information is lost or stolen.
Axon Responsibility	Incident management and response processes are documented, maintained, and communicated to appropriate management and Axon personnel. Compliance liaisons and incident response contacts are maintained to support rapid engagement in the event of an emergency. Incident response plans and procedures are implemented and include detail surrounding the handling of forensic and evidentiary data.
Implementation Support	**IR-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-61; NIST 800-100

5.3.1 Reporting Security Events	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: RC.CO-2 **NIST**: IR-4(1), IR-6, IR-6(1), IR-6(2), IR-7, IR-7(1), IR-7(2), IR-8, PE-17
SOC Report	SEF-02-01; SEF-04-01
Agency Responsibility	Agencies are responsible for establishing incident response capabilities and must report to Axon if they believe an unauthorized third party may be using their account or their content, or if their account information is lost or stolen. Appendix F.1: Security Incident Response Form of the CJIS Security Policy v5.9 provides a template to assist in meeting this control.
Axon Responsibility	Axon will notify customer administrators registered on Axon Cloud Services within 48 hours of a confirmed incident. Authorities will be notified through Axon's established channels and timelines. Axon employees are trained on and made aware of procedures to inform the Axon Information Security Team in the event of an identified security event or weakness.
Implementation Support	**IR-4**: NIST 800-61; NIST 800-86; NIST 800-101; NISTIR 7599 **IR-6**: NIST 800-61 **IR-7**: NISTIR 7599 **IR-8**: NIST 800-61 **PE-17**: NIST 800-46

5.3.2 Management of Security Incidents	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: RC.CO-1 **NIST**: IR-1, IR-8
SOC Report	SEF-01-01; SEF-02-01; SEF-04-01
Agency Responsibility	Agencies are responsible for establishing incident response capabilities and must report to Axon if they believe an unauthorized third party may be using their account or their content, or if their account information is lost or stolen.
Axon Responsibility	Axon maintains security incident response procedures and capabilities for Axon Cloud Services. Details can be found within Axon's SOC 2+ report upon request.
Implementation Support	**IR-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-61; NIST 800-100 **IR-8**: NIST 800-61

5.3.2.1 Incident Handling	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: RC.RP-1 **NIST**: IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8
SOC Report	SEF-02-01; SEF-05-01
Agency Responsibility	Agencies are responsible for establishing incident response capabilities and must report to Axon if they believe an unauthorized third party may be using their account or their content, or if their account information is lost or stolen.
Axon Responsibility	Axon maintains security incident response procedures and capabilities for Axon Cloud Services. Details can be found within Axon's SOC 2+ report upon request.
Implementation Support	**IR-4**: NIST 800-61; NIST 800-86; NIST 800-101; NISTIR 7599 **IR-8**: NIST 800-61

5.3.2.2 Collection of Evidence	
Control Statement	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).
Control Owner	Shared
Mapping	**CSF**: RS.AN-3 **NIST**: IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8
SOC Report	SEF-04-01
Agency Responsibility	Agencies are responsible for establishing incident response capabilities and must report to Axon if they believe an unauthorized third party may be using their account or their content, or if their account information is lost or stolen.
Axon Responsibility	Axon maintains security incident response procedures and capabilities for Axon Cloud Services, which include requirements to collect and maintain appropriate evidence, when necessary.
Implementation Support	**IR-4**: NIST 800-61; NIST 800-86; NIST 800-101; NISTIR 7599 **IR-8**: NIST 800-61

5.3.3 Incident Response Training	
Control Statement	The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.
Control Owner	Shared
Mapping	**CSF**: RS.CO-1 **NIST**: IR-2, IR-3
SOC Report	GRM-03-01; CJI-5.2.1-01
Agency Responsibility	Agencies are responsible for establishing incident response capabilities and including general incident response roles and responsibilities in security awareness training.
Axon Responsibility	The Axon security awareness training for Cloud Services includes security incident response roles and responsibilities, including reporting expectations. Details can be found within Axon's SOC 2+ report upon request.
Implementation Support	**IR-2**: NIST 800-50 **IR-3**: NIST 800-84; NIST 800-115

5.3.4 Incident Monitoring	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: RS.CO-5 **NIST**: IR-5
SOC Report	SEF-05-01; TCC-7.2-01; TSC-7.4-01
Agency Responsibility	Agencies are responsible for establishing incident response capabilities and tracking and documenting incidents. Agencies must report to Axon if they believe an unauthorized third party may be using their account or their content, or if their account information is lost or stolen.
Axon Responsibility	Axon maintains security incident response procedures and capabilities for Axon Cloud Services. Axon internally tracks and documents all security incidents to ensure proper remediation. Details can be found within Axon's SOC 2+ report upon request.
Implementation Support	**IR-5**: NIST 800-61

CJIS Security Policy Area 4 - Auditing and Accountability

5.4 Auditing and Accountability	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.PT-1 **NIST**: AU-1
SOC Report	IAM-01-01; IAM-02-01
Agency Responsibility	Agencies must document and execute their implementation of audit monitoring, analysis, and reporting. Within the Axon Cloud Services, detailed usage and access reports are available for agencies to monitor their accounts.
Axon Responsibility	Within the Axon Cloud Services application, logs are generated and secured that detail all access to evidence data, and robust evidence audit reports are available to customers.
Implementation Support	**AU-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-50; NIST 800-100

5.4.1 Auditable Events and Content (Information Systems)	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.PT-1 **NIST**: AC-9, AU-2, AU-3, AU-3(1), AU-6, AU-6(1), AU-6(3), AU-12, CA-7
SOC Report	IVS-01-02
Agency Responsibility	N/A
Axon Responsibility	In alignment with the Axon Information Security program, Axon Cloud Services systems are configured to log all required events and more to a central logging system. Additionally, within the Axon Cloud Services application, logs are generated and secured that detail all access to evidence data, and robust evidence audit reports are available to customers.
Implementation Support	**AC-9**: N/A **AU-2**: NIST 800-92 **AU-3**: NISTIR 8062 **AU-6**: NIST 800-86; NIST 800-101 **AU-12**: N/A **CA-7**: NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8011; NISTIR 8062

5.4.1.1 Events	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.PT-1 **NIST**: AC-9, AU-2, AU-12, CA-7
SOC Report	IVS-01-02
Agency Responsibility	Within the Axon Cloud Services, detailed usage and access reports are available for agencies to monitor their accounts. Agencies may ingest logs originating from Axon Cloud Services utilizing the Partner API or through a manual process.
Axon Responsibility	In alignment with the Axon Information Security program, Axon Cloud Services systems are configured to log all required events and more to a central logging system. Additionally, within the Axon Cloud Services application, logs are generated and secured that detail all access to evidence data, and robust evidence audit reports are available to customers.
Implementation Support	**AC-9**: N/A **AU-2**: NIST 800-92 **AU-12**: N/A **CA-7**: NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8011; NISTIR 8062

5.4.1.1.1 Content	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.PT-1 **NIST**: AU-12
SOC Report	IVS-01-02
Agency Responsibility	Within the Axon Cloud Services, detailed usage and access reports are available for agencies to monitor their accounts. Agencies may ingest logs originating from Axon Cloud Services utilizing the Partner API or through a manual process.
Axon Responsibility	Axon audit trails capture the required content.
Implementation Support	**AU-12**: N/A

5.4.2 Response to Audit Processing Failures	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.PT-1 **NIST**: AU-05, AU-5(2)
SOC Report	SEF-02-01
Agency Responsibility	Within the Axon Cloud Services application, detailed usage and access reports are available for agencies to monitor their accounts.
Axon Responsibility	Controls are established to alert Axon of any log collection or processing failures.
Implementation Support	**AU-05**: N/A

5.4.3 Audit Monitoring, Analysis, and Reporting	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.PT-1 **NIST**: AU-6, AU-6(1), AU-6(3), AU-7, CA-7, SI-4
SOC Report	SEF-02-01
Agency Responsibility	Agencies must document and execute their implementation of audit monitoring, analysis, and reporting. Within the Axon Cloud Services application, detailed usage and access reports are available for agencies to monitor their accounts.
Axon Responsibility	Axon employs advanced detection and analysis capabilities of system events for Axon Cloud Services. This includes automated detection and alerts for unusual activity or attacks. The Axon internal SOC conducts real time assessment and weekly review of events within the Axon environment.
Implementation Support	**AU-6**: NIST 800-86; NIST 800-101 **AU-7**: N/A **CA-7**: NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8011; NISTIR 8062 **SI-4**: NIST 800-61; NIST 800-83; NIST 800-92; NIST 800-94; NIST 800-137

5.4.4 Time Stamps	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.PT-1 **NIST**: AU-8, SC-45(1)
SOC Report	IVS-01-02; IVS-03-01
Agency Responsibility	N/A
Axon Responsibility	The Axon Cloud Services central logging system collects event generation time and event received time. All systems are synchronized to an internal clock. Customer logs within Axon Cloud Services also include timestamps synchronized to an internal clock.
Implementation Support	**AU-8**: N/A **SC-45**: N/A

5.4.5 Protection of Audit Information	
Control Statement	The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.
Control Owner	Axon
Mapping	**CSF**: PR.PT-1 **NIST**: AU-9, AU-9(4)
SOC Report	IAM-01-01
Agency Responsibility	N/A
Axon Responsibility	In alignment with the Axon Information Security program, Axon Cloud Services systems are configured to log all required events and more to a central logging system. The central logging system protects logs from unauthorized access, modification, and deletion. Additionally, the Axon Cloud Services platform creates and maintains tamper-proof evidence audit records including the when, who, and what for each evidence file. These records cannot be edited or changed, even by account administrators.
Implementation Support	**AU-9**: FIPS 140-2; FIPS 180-4; FIPS 202

5.4.6 Audit Record Retention	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.PT-1 **NIST**: AU-4, AU-5(1), AU-9(2), AU-11
SOC Report	SEF-02-01
Agency Responsibility	N/A
Axon Responsibility	Axon Cloud Services system central log data is maintained for at least one (1) year. Evidence and user access logs within Axon Cloud Services are retained for at least one (1) year, even after evidence deletion.
Implementation Support	**AU-4**: N/A **AU-5**: N/A **AU-9**: FIPS 140-2; FIPS 180-4; FIPS 202 **AU-11**: N/A

5.4.7 Logging NCIC and III Transactions	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.PT-1 **NIST**: AU-4, AU-11
SOC Report	Agency
Agency Responsibility	Agencies are responsible for implementing controls to capture and retain applicable NCIC and III transaction logs.
Axon Responsibility	Not applicable to Axon Cloud Services as Axon does not directly conduct NCIC and III transactions. Axon solutions receiving NCIC and III transactions are routed via CommSys integration.
Implementation Support	**AU-4**: N/A **AU-11**: N/A

CJIS Security Policy Area 5 - Access Control

5.5 Access Control	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: ID.GV-1 **NIST**: AC-1
Agency Responsibility	Agencies are responsible for establishing Access Control policies and procedures.
Axon Responsibility	Axon maintains Access Control policies and practices for Axon Cloud Services.
Implementation Support	**AC-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100; NISTIR 7874

5.5.1 Account Management	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-1; PR.AC-4 **NIST**: AC-2, AC-5, IR-8
SOC Report	IAM-02-01; IAM-02-02; IAM-02-04
Agency Responsibility	Agencies are responsible for implementing this control for their user access into Axon Cloud Services. Axon Cloud Services allow for customers to directly administer user accounts.
Axon Responsibility	Axon maintains account management policies and practices for Axon Cloud Services systems including at least quarterly account validation.
Implementation Support	**AC-2**: NIST 800-162; NIST 800-178 **AC-5**: N/A **IR-8**: NIST 800-61

5.5.2 Access Enforcement	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-4 **NIST**: AC-2, AC-2(1), AC-2(7), AC-3, AC-3(3), AC-3(4), AC-5, AC-6(1), AC-6(2), AC-12(1), SC-23(1), SC-23(3)
SOC Report	IAM-02-01; IAM-02-03; IAM-04-01
Agency Responsibility	Agencies are responsible for implementing this control for their user access into Axon Cloud Services. Within Axon Cloud Services roles and permissions are customizable by customers. Default roles are included for customers upon customer tenant creation. These are locked roles and cannot be modified. All other roles are customizable by customers.
Axon Responsibility	Axon has documented and implemented logical access controls to enforce session control, authorization, multi-factor and remote access requirements. Individuals are assigned unique User IDs when accessing Axon systems. Axon account management practices and implementation is designed according to the principle of least privilege.
Implementation Support	**AC-2**: NIST 800-162; NIST 800-178 **AC-3**: NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-162; NISTIR 7874 **AC-5**: N/A **AC-6**: N/A **AC-12**: N/A **SC-23**: NIST 800-52; NIST 800-77; NIST 800-95; NIST 800-113

5.5.2.1 Least Privilege	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-4 **NIST**: AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
SOC Report	IAM-02-01; IAM-02-02
Agency Responsibility	Agencies are responsible for implementing this control for their user access into Axon Cloud Services. Axon Cloud Services allow for customers to directly administer user accounts.
Axon Responsibility	Axon account management practices and implementation are designed according to the principle of least privilege.
Implementation Support	**AC-2**: NIST 800-162; NIST 800-178 **AC-5**: N/A **AC-6**: N/A **AC-10**: N/A **RA-5**: NIST 800-40; NIST 800-70; NIST 800-115; NIST 800-126; NISTIR 7788; NISTIR 8023

5.5.2.2 System Access Control	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-4 **NIST**: AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
SOC Report	IAM-02-03; CJI-5.5.2; HRS-11-01
Agency Responsibility	Agencies are responsible for implementing this control for their user access into the Axon Cloud Services application. Axon Cloud Services allow for granular permissions to application features and data as well as restricting concurrent active sessions.
Axon Responsibility	Axon account management practices and implementation are designed according to the principle of least privilege. Systems and connectivity are restricted to authorized individuals and applications. Axon Cloud Services restrict the use of concurrent active sessions.
Implementation Support	**AC-2**: NIST 800-162; NIST 800-178 **AC-5**: N/A **AC-6**: N/A **AC-10**: N/A **RA-5**: NIST 800-40; NIST 800-70; NIST 800-115; NIST 800-126; NISTIR 7788; NISTIR 8023

5.5.2.3 Access Control Criteria	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-4 **NIST**: AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
SOC Report	IAM-02-01; IAM-04-01
Agency Responsibility	Axon Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence including: • Multiple multi-factor authentication options (one-time code via SMS, email, or phone call-back) • Role-based permission management • Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) • Restrict access to defined IP ranges (limit access to approved office locations) Agencies are required to enforce technical and administrative controls to ensure personnel owned information systems are not used to access Axon Cloud Services.
Axon Responsibility	Axon Cloud Services system access control mechanisms are maintained in compliance with the specific CJIS security requirements. Access control to the system is limited to authorized users and uses multiple factors for authentication.
Implementation Support	**AC-2**: NIST 800-162; NIST 800-178 **AC-5**: N/A **AC-6**: N/A **AC-10**: N/A **RA-5**: NIST 800-40; NIST 800-70; NIST 800-115; NIST 800-126; NISTIR 7788; NISTIR 8023

5.5.2.4 Access Control Mechanisms	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-4 **NIST**: AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
SOC Report	EKM-01-01; HRS-11-01; IAM-02-01; IAM-04-01; TCC-5.1-01
Agency Responsibility	Axon Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence including: • Multiple multi-factor authentication options (one-time code via SMS, email, or phone call-back) • Role-based permission management • Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) • Restrict access to defined IP ranges (limit access to approved office locations) Agencies are required to enforce technical and administrative controls to ensure personnel owned information systems are not used to access Axon Cloud Services.
Axon Responsibility	Axon Cloud Services system access control mechanisms are maintained in compliance with the specific CJIS security requirements. Access control to the system is limited to authorized users and uses multiple factors for authentication. Evidence data is encrypted at rest and in transit. Axon maintains key management practices for managing the encryption keys.
Implementation Support	**AC-2**: NIST 800-162; NIST 800-178 **AC-5**: N/A **AC-6**: N/A **AC-10**: N/A **RA-5**: NIST 800-40; NIST 800-70; NIST 800-115; NIST 800-126; NISTIR 7788; NISTIR 8023

5.5.3 Unsuccessful Login Attempts	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6 **NIST**: AC-7, IA-5(1)
SOC Report	HRS-11-01; IAM-04-01; TCC-5.1-01
Agency Responsibility	Agencies are required to enforce technical and administrative controls to restrict access to Axon Cloud Services. Axon Cloud Services restrict consecutive invalid login attempts as well as account lockout periods in accordance with CJIS Policy requirements. Axon Cloud Services allow for agency administrators to customize these controls for their tenants.
Axon Responsibility	Axon Cloud Services access control mechanisms are maintained in compliance with the specific CJIS security requirements and enforce user lockouts or deny attempts from malicious-appearing IPs.
Implementation Support	**AC-7**: NIST 800-63; NIST 800-124 **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040

5.5.4 System Use Notification	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6 **NIST**: AC-8, AC-11(1), AC-22
SOC Report	AAC-03-01; CJI-5.5.4
Agency Responsibility	Agencies are required to enforce technical and administrative controls to restrict access to Axon Cloud Services. Axon Cloud Services allow agencies the ability to configure and customize the system use notification language.
Axon Responsibility	Axon Cloud Services systems implements an approved system use notification in compliance with the specific CJIS security requirement.
Implementation Support	**AC-8**: N/A **AC-11**: N/A **AC-22**: N/A

5.5.5 Session Lock	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-7 **NIST**: AC-11
SOC Report	HRS-11-01; TCC-5.1-01
Agency Responsibility	Agencies are required to enforce technical and administrative controls to restrict access to Axon Cloud Services. Axon Cloud Services allow agencies the ability to configure and customize the inactivity period lockout in accordance with CJIS Policy requirements.
Axon Responsibility	Axon Cloud Services system administration access control mechanisms are maintained in compliance with the specific CJIS security requirements.
Implementation Support	**AC-11**: N/A

5.5.6 Remote Access	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-3 **NIST**: AC-17, AC-17(3), AC-17(4), AC-17(6)
SOC Report	HRS-11-01; TCC-5.1-01
Agency Responsibility	Agencies are responsible for authorizing and monitoring the methods in which remote access is granted to their tenant within Axon Cloud Services. Axon Cloud Services supports several authentication options including multi-factor authentication, Single Sign-On (SSO), and API tokens.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services that limit remote access to only required individuals and require at least two factors for authentication. Axon maintains Secure Locations at the Arizona and Washington facilities and permits remote access for the viewing of sensitive data outside of Axon Secure Locations only for compelling needs.
Implementation Support	**AC-17**: NIST 800-46; NIST 800-77; NIST 800-113; NIST 800-114; NIST 800-121; NISTIR 7966

5.5.6.1 Personally Owned Information Systems	
Control Statement	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).
Control Owner	Shared
Mapping	**CSF**: ID.AM-4 **NIST**: AC-17
SOC Report	HRS-11-01; MOS-06-01
Agency Responsibility	Axon Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence and prohibit the usage of personally owned information systems including: • Application permission management (for example, allow specific users to use the web-based interface, but not the mobile application) • Restrict access to defined IP ranges (limit access to approved office locations) Agencies are required to enforce technical and administrative controls to restrict access to Axon Cloud Services.
Axon Responsibility	Axon prohibits the usage of personally owned information systems to access, process, store, or transmit CJI.
Implementation Support	**AC-17**: NIST 800-46; NIST 800-77; NIST 800-113; NIST 800-114; NIST 800-121; NISTIR 7966

5.5.6.2 Publicly Accessible Computers	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-3 **NIST**: AC-17, AC-22
SOC Report	HRS-08-01; HRS-11-01
Agency Responsibility	Axon Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence including restricting access to a defined IP ranges which limits access to approved locations.
Axon Responsibility	Axon Cloud Services back-end system administration is prohibited from publicly accessible computers.
Implementation Support	**AC-17**: NIST 800-46; NIST 800-77; NIST 800-113; NIST 800-114; NIST 800-121; NISTIR 7966 **AC-22**: N/A

CJIS Security Policy Area 6 - Identification and Authentication

5.6 Identification and Authentication	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-1 **NIST**: IA-1
SOC Report	TCC-5.2-02
Agency Responsibility	Agencies are responsible for properly identifying and vetting system users prior to granting them access to Axon Cloud Services through appropriate policies and procedures.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services for identifying and authenticating users before allowing access.
Implementation Support	**IA-1**: FIPS 201; NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-100; NISTIR 7874

5.6.1 Identification Policy and Procedures	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6 **NIST**: IA-1, IA-2, IA-2(5)
SOC Report	HRS-11-01; IAM-02-02; IAM-02-03; IAM-02-04; TCC-5.2-02
Agency Responsibility	Agencies are responsible for properly identifying and vetting system users prior to granting them access to Axon Cloud Services through appropriate policies and procedures.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services for identifying and authenticating users before allowing access.
Implementation Support	**IA-1**: FIPS 201; NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-100; NISTIR 7874 **IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966

5.6.2 Authentication Policy and Procedures	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-6 **NIST**: IA-1, IA-2, IA-2(8), IA-2(9), IA-3
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.
Axon Responsibility	N/A
Implementation Support	**IA-1**: FIPS 201; NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-100; NISTIR 7874 **IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-3**: N/A

5.6.2.1 Standard Authenticators	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-7 **NIST**: IA-5, IA-5(1), IA-5(5), IA-6
SOC Report	TCC-5.1-01
Agency Responsibility	Axon Cloud Services do not use a PIN for authentication.
Axon Responsibility	Axon Cloud Services do not use a PIN for authentication.
Implementation Support	**IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **IA-6**: N/A

5.6.2.1.1 Password	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6 **NIST**: IA-5, IA-5(1)
SOC Report	IAM-04-01; TCC-5.1-01
Agency Responsibility	Agencies must address this requirement by selecting which standard to use.
Axon Responsibility	Axon Cloud Services use the basic password standards.
Implementation Support	**IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040

5.6.2.1.1.1 Basic Password Standards	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6 **NIST**: IA-5, IA-5(1)
SOC Report	TCC-5.1-01
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services. Axon Cloud Services provide many security features and capabilities including customizable password length and complexity requirements, strong encryption to protect data in transit, and masking of password in the entry form.
Axon Responsibility	Axon Cloud Services password complexity requirements are maintained in compliance with the basic password standards.
Implementation Support	**IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040

5.6.2.1.1.2 Advanced Password Standards	
Control Statement	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. 10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6; PR.AC-7 **NIST**: IA-5, IA-5(1)
SOC Report	TCC-5.1-01
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services. Axon Cloud Services provide many security features and capabilities including customizable password length and complexity requirements, strong encryption to protect data in transit, and masking of password in the entry form.
Axon Responsibility	Axon Cloud Services password complexity requirements are maintained in compliance with the basic password standards.
Implementation Support	**IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040

5.6.2.1.2 Personal Identification Number (PIN)	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6 **NIST**: IA-5, IA-5(1)
SOC Report	TCC-5.1-01
Agency Responsibility	N/A; Axon Cloud Services do not use a PIN for authentication.
Axon Responsibility	N/A; Axon Cloud Services do not use a PIN for authentication.
Implementation Support	**IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040

5.6.2.1.3 One-time Passwords (OTP)	
Control Statement	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
Control Owner	Shared
Mapping	**CSF**: PR.AC-7 **NIST**: IA-2(1), IA-2(2), IA-2(6), IA-2(8), IA-2(12), IA-5(1), IA-5(5), IA-12(4), SC-37, SC-37(1)
SOC Report	TCC-5.1-01
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services. Axon Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence, including time-based one-time passwords (TOTP) as a required secondary authenticator. TOTP requirements include a minimum of six (6) numeric characters.
Axon Responsibility	Axon Cloud Services use a time-based one-time password (TOTP) as a required secondary authenticator for some administrative access. TOTP requirements include a minimum of six (6) numeric characters.
Implementation Support	**IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **IA-12**: FIPS 201; NIST 800-63; NIST 800-63A **SC-37**: NIST 800-57-1; NIST 800-57-2; NIST 800-57-3

5.6.2.2 Advanced Authentication	
Control Statement	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., 4. passphrase or user-specific PIN).
Control Owner	Shared
Mapping	**CSF**: PR.AC-7 **NIST**: IA-2(1), IA-2(2), IA-2(6), IA-2(13), IA-3(1), IA-5(2), MA-4, SC-37, SC-37(1)
SOC Report	TCC-5.1-01
Agency Responsibility	Axon Cloud Services do not use user-based certifications for authentication.
Axon Responsibility	Axon Cloud Services requires at least two-factor authentication for all system administration access IAW Appendix G.5 Administrator Accounts for Least Privilege and Separation of Duties. Axon Cloud Services do not utilize user-based certifications for authentication.
Implementation Support	**IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-3**: N/A **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **MA-4**: FIPS 140-2; FIPS 197; FIPS 201; NIST 800-63; NIST 800-88 **SC-37**: NIST 800-57-1; NIST 800-57-2; NIST 800-57-3

5.6.2.2.1 Advanced Authentication Policy and Rationale	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-7 **NIST**: IA-2(1), IA-2(2), IA-2(6), IA-3(1), IA-5(2), MA-4
SOC Report	TCC-5.1-01
Agency Responsibility	Agencies are responsible for determining when Advanced Authentication must be used on Axon Cloud Services by establishing an appropriate policy and rationale. Axon Cloud Services provide many security features and capabilities to enable customers to securely manage digital evidence, including multiple multi-factor authentication options (one-time code via SMS, email, or phone call-back) and the ability to restrict access to defined IP ranges (limit access to approved office locations)
Axon Responsibility	System administration access to Axon Cloud Services requires at least two-factor authentication.
Implementation Support	**IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-3**: N/A **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **MA-4**: FIPS 140-2; FIPS 197; FIPS 201; NIST 800-63; NIST 800-88

5.6.3 Identifier and Authenticator Management	
Control Statement	The agency shall establish identifier and authenticator management processes.
Control Owner	Shared
Mapping	**CSF**: PR.AC-1 **NIST**: IA-4, IA-4(4), IA-5, IA-5(8), IA-8, IA-12(1)
SOC Report	IAM-02-01; IAM-04-01
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services for Identifier and Authenticator management.
Implementation Support	**IA-4**: FIPS 201; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78 **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **IA-8**: FIPS 201; NIST 800-63; NIST 800-79; NIST 800-116; NISTIR 8062 **IA-12**: FIPS 201; NIST 800-63; NIST 800-63A

5.6.3.1 Identifier Management	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-6 **NIST**: AC-2(3), IA-4, IA-4(4), IA-5(8), IA-8, IA-12(1), IA-12(4)
SOC Report	IAM-02-02; IAM-02-04; IAM-04-01; TCC-5.2-02
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services for Identifier and Authenticator management through Axon's Information Security Program. Additionally, all users are required to have unique login credentials.
Implementation Support	**AC-2**: NIST 800-162; NIST 800-178 **IA-4**: FIPS 201; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78 **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **IA-8**: FIPS 201; NIST 800-63; NIST 800-79; NIST 800-116; NISTIR 8062 **IA-12**: FIPS 201; NIST 800-63; NIST 800-63A

5.6.3.2 Authenticator Management	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-1 **NIST**: IA-5, IA-5(6), IA-5(8)
SOC Report	IAM-02-04; IAM-04-01; TCC-5.1-01
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services for Identifier and Authenticator management through the Information Security Program.
Implementation Support	**IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040

5.6.4 Assertions	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-7 **NIST**: IA-2(12), IA-8(1), IA-8(2)
SOC Report	HRS-11-01; TCC-5.1-01
Agency Responsibility	Axon Cloud Services allow the option for agencies to use single sign-on with a federated identity service. This feature uses the industry standard SAML protocol.
Axon Responsibility	Axon Cloud Services do not remotely authenticate Axon personnel to Axon Cloud Services. As such, assertion mechanisms are not used.
Implementation Support	**IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-8**: FIPS 201; NIST 800-63; NIST 800-79; NIST 800-116; NISTIR 8062

CJIS Security Policy Area 7 - Configuration Management

5.7.1 Access Restrictions for Changes	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.IP-3 **NIST**: CM-3, CM-3(2), CM-4, CM-4(2), CM-5(5), CM-5(6), CM-6, CM-9, MA-2, MA-5, SA-10
SOC Report	GRM-01-01
Agency Responsibility	Agency administrators rarely have actionable requirements for planned updates and security patches. In the event of scheduled routine or planned maintenance requires actions by the agency administrator, they will be notified via email at least sixty days prior to the maintenance; for emergency maintenance agency administrators may only be notified less than one week in advance.
Axon Responsibility	Axon maintains a planned maintenance window which occurs on Tuesdays from 2100 PST to 2200 PST and should not result in service disruptions.
Implementation Support	**CM-3**: NIST 800-124; NIST 800-128; NISTIR 8062 **CM-4**: NIST 800-128 **CM-5**: FIPS 140-2; FIPS 186-4 **CM-6**: NIST 800-70; NIST 800-126; NIST 800-128; US Government Configuration Baselines; National Checklist Repository **CM-9**: NIST 800-128 **MA-2**: NISTIR 8023 **MA-5**: N/A **SA-10**: FIPS 140-2; FIPS 180-4; FIPS 202; NIST 800-128

5.7.1.1 Least Functionality	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.IP-1 **NIST**: CM-2, CM-3, CM-6, CM-7, CM-7(1), CM-7(2), CM-7(3), CM-7(4), CM-7(5), CM-8(3), CM-10, CM-11, SA-4(9), SA-9(2)
SOC Report	GRM-01-01; IVS-06-01
Agency Responsibility	Agencies are responsible for restricting and controlling changes made by agency personnel to their Axon Cloud Services.
Axon Responsibility	Axon designs and maintains the Axon Cloud Services infrastructure under the principle of least functionality.
Implementation Support	**CM-2**: NIST 800-124; NIST 800-128 **CM-3**: NIST 800-124; NIST 800-128; NISTIR 8062 **CM-6**: NIST 800-70; NIST 800-126; NIST 800-128; US Government Configuration Baselines; National Checklist Repository **CM-7**: FIPS 140-2; FIPS 180-4; FIPS 186-4; FIPS 202; NIST 800-167 **CM-8**: NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NISTIR 8062 **CM-10**: N/A **CM-11**: N/A **SA-4**: FIPS 140-2; FIPS 201; NIST 800-23; NIST 800-35; NIST 800-36; NIST 800-37; NIST 800-64; NIST 800-70; NIST 800-73; NIST 800-137; NIST 800-161; NISTIR 7539; NISTIR 7622; NISTIR 7676; NISTIR 7870; NISTIR 8062 **SA-9**: NIST 800-35; NIST 800-161

5.7.1.2 Network Diagram	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: ID.AM-3 **NIST**: CA-3, CA-9, SC-7(4)
SOC Report	IVS-13-01
Agency Responsibility	Agencies are responsible for maintaining their own system diagram that contains the Axon Cloud Services connection. Appendix C of the CJIS Security Policy v5.9 provides additional guidance on Network Topology Diagrams.
Axon Responsibility	Axon maintains a current system diagram for Axon Cloud Services. A copy of Axon's Network and Security Architecture Diagram can be found in **Attachment B: Network and Security Architecture Diagram**.
Implementation Support	**CA-3**: FIPS 199; NIST 800-47 **CA-9**: NIST 800-124; NISTIR 8023 **SC-7**: FIPS 199; NIST 800-41; NIST 800-77

5.7.2 Security of Configuration Documentation	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-4 **NIST**: CM-2, CM-3(7), CM-5, CM-5(1), CM-8, CM-8(1), CM-9, SA-5
SOC Report	GRM-01-01; IAM-04-01
Agency Responsibility	Agencies are responsible for maintaining appropriate safeguards to ensure access to system documentation is limited to authorized personnel.
Axon Responsibility	Axon maintains appropriate safeguards to ensure access to system documentation is limited to authorized personnel.
Implementation Support	**CM-2**: NIST 800-124; NIST 800-128 **CM-3**: NIST 800-124; NIST 800-128; NISTIR 8062 **CM-5**: FIPS 140-2; FIPS 186-4 **CM-8**: NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NISTIR 8062 **CM-9**: NIST 800-128 **SA-5**: N/A

CJIS Security Policy Area 8 - Media Protection

MP-1 Policy and Procedures	
Control Statement	a. Develop, document, and disseminate to authorized individuals: 1. Agency-level media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls. b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and c. Review and update the current media protection: 1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and 2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.
Control Owner	Agency
CSF Mapping	ID.GV-1; PR.PT-2
SOC Report	GRM-01-01
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding secure handling of data.
Axon Responsibility	Axon maintains policies and procedures for Axon Cloud Services related to Media Protection. The Axon CISO reviews and authorizes Media Protection policies and procedures annually.
Implementation Support	NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100
Related Controls	PS-8, SI-12

MP-2 Media Access	
Control Statement	Restrict access to digital and non-digital media to authorized individuals.
Control Owner	Shared
CSF Mapping	PR.DS-2; PR.PT-2
SOC Report	EKM-03-01
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding secure handling of data.
Axon Responsibility	Axon ensures customer data, to include CJI, is only stored and processed within ACS; access is limited to CJIS cleared Axon personnel with a designated business need from Axon's Secure Locations.
Implementation Support	FIPS 199; NIST 800-111
Related Controls	AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SI-12

MP-3 Media Marking	
Control Statement	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations or controlled areas.
Control Owner	Agency
CSF Mapping	PR.DS-2; PR.PT-2
SOC Report	T17-8.2.2
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding secure handling of data.
Axon Responsibility	Axon provides customers with Administrator Guides on data labeling and categorization functionality within ACS. Axon does not utilize removable media for storage of customer data requiring media marking.
Implementation Support	FIPS 199
Related Controls	CP-9, MP-5, SI-12

MP-4 Media Storage	
Control Statement	a. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
Control Owner	Shared
CSF Mapping	PR.DS-2
SOC Report	EKM-03-01
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding secure handling of data.
Axon Responsibility	Axon ensures all customer data, to include CJI, is stored and processed within ACS; removal to local devices or removal media is not permitted. Axon does not store or permit the creation of physical customer data. Axon approved systems used to access customer data within ACS are safeguarded in Axon Secure Locations and sanitized IAW MP-6 Media Sanitization. ACS inherits media sanitization and disposal controls from its cloud service provider. Sanitization and disposal activities are conducted IAW NIST 800-88 and NSA Media Destruction Guidance.
Implementation Support	FIPS 199; NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-111
Related Controls	AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SI-12

MP-5 Media Transport	
Control Statement	a. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in Section 5.10.1.2 of this Policy. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel; b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas; c. Document activities associated with the transport of system media; and d. Restrict the activities associated with the transport of system media to authorized personnel.
Control Owner	Agency
CSF Mapping	PR.DS-2
SOC Report	Out of Scope
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding secure handling of data.
Axon Responsibility	Axon does not store or permit the creation of physical customer data, to include CJI. All digital customer data is encrypted in transit over public networks using a robust TLS 1.2 implementation with 256 Bit Perfect Forward Secrecy. Axon does not utilize local devices or removable media for transport of customer data.
Implementation Support	FIPS 199; NIST 800-60-1; NIST 800-60-2
Related Controls	AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28

MP-6 Media Sanitization	
Control Statement	a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
Control Owner	Shared
CSF Mapping	PR.DS-1; PR.DS-3; PR.IP-6
SOC Report	DCS-05; DSI-07
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding electronic media sanitization and disposal of data outside of Axon Cloud Services.
Axon Responsibility	Axon Cloud Services inherits media sanitization and disposal controls from its cloud service provider. Sanitization and disposal activities are conducted IAW NIST 800-88 and NSA Media Destruction Guidance. Upon termination of contract, Certificates of Destruction can be requested from Axon Customer Success. Axon maintains practices for sanitizing and disposing of its internal electronic media. Including: 1. Data destruction and removal activities should be logged in an auditable format to ensure important devices are not missed. 2. The transfer of a workstation to a new owner requires full wiping of the previous owner's data. 3. Data storage devices must be fully wiped or destroyed before disposal. 4. Data destruction and wiping techniques must ensure that a determined attacker with moderate capabilities cannot recover the data.
Implementation Support	**MP-6**: FIPS 199; NIST 800-60-1; NIST 800-60-2; NIST 800-88; NIST 800-124; NISTIR 8023
Related Controls	AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, SI-12, SR-11

MP-7 Media Use	
Control Statement	a. Restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls (examples below); and b. Prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information; and c. Prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.
Control Owner	Shared
CSF Mapping	PR.DS-2; PR.PT-2
SOC Report	EKM-03-01
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding secure handling of data.
Axon Responsibility	Axon maintains policies and procedures for ACS that limit access to only approved Axon personnel from Axon Secure Locations on approved, assigned systems requiring at least two factors of authentication. Axon prohibits the usage of personally owned information systems to access, process, store, or transmit CJI.
Implementation Support	FIPS 199; NIST 800-111
Related Controls	AC-19, AC-20, PL-4

CJIS Security Policy Area 9 - Physical Protection

5.9 Physical Protection	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: ID.GV-1 **NIST**: PE-1
SOC Report	CC6.4; DCS-02; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for documenting and implementing policies regarding physical protection.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services related to physical protection.
Implementation Support	**PE-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100

5.9.1 Physically Secure Location	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-1
SOC Report	CC6.4; CC6.5; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for maintaining controlled areas IAW this control.
Axon Responsibility	Axon maintains controlled areas at both its Arizona and Washington locations IAW this control.
Implementation Support	**PE-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100

5.9.1.1 Security Perimeter	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-1
SOC Report	DCS-02; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for maintaining a secure physical perimeter.
Axon Responsibility	Axon defines and controls the physically secure perimeter for Axon facilities.
Implementation Support	**PE-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100

5.9.1.2 Physical Access Authorizations	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: MA-4(7), MA-5, PE-2, PE-2(1)
SOC Report	CC6.4; CC6.5; DCS-09; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for restricting and controlling physical access to secure locations, as determined and managed by agencies, to support the use of Axon Cloud Services.
Axon Responsibility	Axon ensures physical access to secure locations is limited to authorized personnel.
Implementation Support	**MA-4**: FIPS 140-2; FIPS 197; FIPS 201; NIST 800-63; NIST 800-88 **MA-5**: N/A **PE-2**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78

5.9.1.3 Physical Access Control	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-3, PE-3(3)
SOC Report	CC6.4; CC6.5; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for restricting and controlling physical access to physical access points.
Axon Responsibility	Axon regularly reviews the specific security practices and audit results documented by underlying infrastructure providers to ensure the highest standards are met. Axon ensures physical access is limited to authorized personnel.
Implementation Support	**PE-3**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-116

5.9.1.4 Access Control for Transmission Medium	
Control Statement	The agency shall control physical access to information system distribution and transmission lines within the physically secure location.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-4
SOC Report	CC6.4; CC6.5; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for restricting and monitoring access to transmission lines within physically secure locations, as determined and managed by agencies, to support the use of Axon Cloud Services.
Axon Responsibility	Axon restricts and monitors access to transmission lines within the physically secure locations used to deliver Axon Cloud Services.
Implementation Support	**PE-4**: N/A

5.9.1.5 Access Control for Display Medium	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-5
SOC Report	CC6.4; CC6.5; T01-11.1.1-01
Agency Responsibility	Agencies should maintain policy and procedure surrounding the devices used to access Axon Cloud Services.
Axon Responsibility	Axon maintains policy and procedure surrounding the devices used to administer Axon Cloud Services.
Implementation Support	**PE-5**: NISTIR 8023

5.9.1.6 Monitoring Physical Access	
Control Statement	The agency shall monitor physical access to the information system to detect and respond to physical security incidents.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-3, PE-5, PE-6, PE-6(1)
SOC Report	CC6.4; CC6.5; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for restricting and controlling physical access to locations managed by agencies to support the use of Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices for monitoring physical access and responding to suspicious events.
Implementation Support	**PE-3**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-116 **PE-5**: NISTIR 8023 **PE-6**: N/A

5.9.1.7 Visitor Control	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-2(3), PE-3
SOC Report	CC6.4; CC6.5; T01-11.1.1-01
Agency Responsibility	Agencies are responsible for restricting and controlling physical access. This includes monitoring and escorting visitors to physically secure locations as determined and managed by agencies to support the use of Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices for controlling visitors to Axon facilities. Visitors are identified with a unique badge only valid for the day of visit. In addition, the purpose of the visit is recorded with reception.
Implementation Support	**PE-2**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78 **PE-3**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-116

5.9.1.8 Delivery and Removal	
Control Statement	The agency shall authorize and control information system-related items entering and exiting the physically secure location.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2; PR.DS-3 **NIST**: PE-8
Agency Responsibility	Agencies are responsible for authorizing and monitoring information system related items entering and leaving physically secure locations, as determined and managed by agencies, to support the use of Axon Cloud Services.
SOC Report	DCS-02; DCS-04; DCS-06; T01-11.1.1-01
Axon Responsibility	Axon maintains policies and practices for controlling information system-related items entering and exiting secure locations.
Implementation Support	**PE-8**: N/A

5.9.2 Controlled Area	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.AC-2 **NIST**: PE-2, PE-5
SOC Report	T01-11.1.1-01
Agency Responsibility	Agencies are responsible for documenting and implementing policies and practices related to physical protection.
Axon Responsibility	Axon maintains policies and practices for Axon Cloud Services related to physical protection.
Implementation Support	**PE-2**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78 **PE-5**: NISTIR 8023

CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity

5.10.1 Information Flow Enforcement	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: ID.AM-3 **NIST**: AC-4, AC-20, AC-20(1), CA-3, CA-9, IA-5(7), SC-7(4), SC-7(8), SC-7(11), SC-10, SC-15, SC-15(1)
SOC Report	IVS-06-01; IVS-13-01
Agency Responsibility	N/A
Axon Responsibility	Axon requires encryption on all connections to Axon Cloud Services over public networks. In addition, Axon maintains a range of capabilities for controlling data flows in Cloud Services, including firewalls, ACLs, proxies, and load balancers.
Implementation Support	**AC-4**: NIST 800-162; NIST 800-178 **AC-20**: FIPS 199 **CA-3**: FIPS 199; NIST 800-47 **CA-9**: NIST 800-124; NISTIR 8023 **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **SC-7**: FIPS 199; NIST 800-41; NIST 800-77 **SC-10**: N/A **SC-15**: N/A

5.10.1.1 Boundary Protection	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.AC-5 **NIST**: AC-20, PE-3(2), SC-5, SC-5(1), SC-5(2), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-7(25), SC-24
SOC Report	IAM-02-01; IVS-06-01; IVS-13-01; SEF-02-01
Agency Responsibility	Agencies are responsible for implementing and maintaining boundary protections, such as network segregation, firewalls, Network Intrusion Detection/Protection, of their local network. Axon hardware deployed to agency networks should be on a segregated VLAN behind the firewall with appropriate ports configured.
Axon Responsibility	Axon maintains controls to protect and monitor the boundaries of Axon Cloud Services. These include firewalls, ACLs, network segmentation, proxies, and intrusion detection systems. Changes to computing resources are detected and monitored. An advanced anti-malware solution is deployed for malware protection on Axon Cloud Services hosts and a host-based IDS/IPS solution is deployed. A web application firewall is deployed on each Axon Cloud Services web servers. Additionally, vulnerability scans are performed on at least monthly basis, and penetration tests are performed regularly.
Implementation Support	**AC-20**: FIPS 199 **PE-3**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-116 **SC-5**: N/A **SC-7**: FIPS 199; NIST 800-41; NIST 800-77 **SC-24**: N/A

5.10.1.2 Encryption	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.DS-5 **NIST**: AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC- 12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-17, SC-28, SC-28(1), SI-7(6)
SOC Report	EKM-03-01; EKM-03-02
Agency Responsibility	Agencies are responsible for meeting encryption requirements for CJI maintained within their environment outside of Axon Cloud Services.
Axon Responsibility	Axon maintains industry standard encryption for evidence data. Stored data in Axon Cloud Services is encrypted with AES 256; data transmitted in Axon Cloud Services is encrypted with 128 bits or stronger Axon securely maintains PKI encryption keys for Axon Cloud Services.
Implementation Support	**AC-17**: NIST 800-46; NIST 800-77; NIST 800-113; NIST 800-114; NIST 800-121; NISTIR 7966 **IA-7**: FIPS 140-2 **MA-4**: FIPS 140-2; FIPS 197; FIPS 201; NIST 800-63; NIST 800-88 SC-8: FIPS 140-2; FIPS 197; NIST 800-52; NIST 800-77; NIST 800-81; NIST 800-113; NIST 800-177; NISTIR 8023 **SC-11**: N/A **SC-12**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-63; NISTIR 7956; NISTIR 7966 **SC-13**: FIPS 140-2 **SC-17**: NIST 800-32; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-63 **SC-28**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-111; NIST 800-124 **SI-7**: FIPS 140-2; FIPS 180-4; FIPS 186-4; FIPS 202; NIST 800-70; NIST 800-147

5.10.1.2.1 Encryption for CJI in Transit	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.DS-2 **NIST**: AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC-12, SC-12(1), SC-12(2), SC-13, SC-28, SC-28(1), SI-7(6)
SOC Report	EKM-03-02
Agency Responsibility	Agencies are responsible for maintaining encryption for data in transit for data being sent to destinations other than Axon Cloud Services.
Axon Responsibility	Data transmitted in Axon Cloud Services is encrypted with 128 bits or stronger. Axon's Cryptographic Module that provides for protection of data in transit is FIPS 140-2 validated: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2878. Axon maintains policies and practices for Axon Cloud Services for encryption key and certificate management. See **Attachment C: FIPS 140-2 Certificate**.
Implementation Support	**AC-17**: NIST 800-46; NIST 800-77; NIST 800-113; NIST 800-114; NIST 800-121; NISTIR 7966 **IA-7**: FIPS 140-2 **MA-4**: FIPS 140-2; FIPS 197; FIPS 201; NIST 800-63; NIST 800-88 **SC-8**: FIPS 140-2; FIPS 197; NIST 800-52; NIST 800-77; NIST 800-81; NIST 800-113; NIST 800-177; NISTIR 8023 **SC-11**: N/A **SC-12**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-63; NISTIR 7956; NISTIR 7966 **SC-13**: FIPS 140-2 **SC-28**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-111; NIST 800-124 **SI-7**: FIPS 140-2; FIPS 180-4; FIPS 186-4; FIPS 202; NIST 800-70; NIST 800-147

5.10.1.2.2 Encryption for CJI at Rest	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.DS-1 **NIST**: AC-17(2), IA-7, SC-12, SC-12(1), SC-12(2), SC-13, SC-28, SC-28(2), SI-7(6)
SOC Report	IPY-05; EKM-03-01
Agency Responsibility	N/A if CJI is maintained within Axon Cloud Services. Agency is responsible for encryption of any CJI at rest stored outside of Axon Cloud Services.
Axon Responsibility	Evidence data stored in Axon Cloud Services is encrypted with AES 256. Axon maintains policies and practices for Axon Cloud Services for encryption key and certificate management. Further details can be found at www.axon.com/trust.
Implementation Support	**AC-17**: NIST 800-46; NIST 800-77; NIST 800-113; NIST 800-114; NIST 800-121; NISTIR 7966 **IA-7**: FIPS 140-2 **SC-12**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-63; NISTIR 7956; NISTIR 7966 **SC-13**: FIPS 140-2 **SC-28**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-111; NIST 800-124 **SI-7**: FIPS 140-2; FIPS 180-4; FIPS 186-4; FIPS 202; NIST 800-70; NIST 800-147

5.10.1.2.3 Public Key Infrastructure (PKI) Technology	
Control Statement	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.
Control Owner	Shared
Mapping	**CSF**: PR.DS-5 **NIST**: IA-2(1), IA-2(2), IA-5(2), IA-5(10), IA-7, IA-8(1), IA-8(5), SC-12(1), SC-12(3), SC-13, SC-17, SC-28(2), SI-7(6)
SOC Report	EKM-01-01; EKM-04-02
Agency Responsibility	N/A
Axon Responsibility	Axon uses PKI to provide server authentication to clients interacting with Axon Cloud Services. Axon's TLS certifications are signed by Rapid SSL. Rapid SSL verifies identity when issuing the certificate.
Implementation Support	**IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **IA-7**: FIPS 140-2 **IA-8**: FIPS 201; NIST 800-63; NIST 800-79; NIST 800-116; NISTIR 8062 **SC-12**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-63; NISTIR 7956; NISTIR 7966 **SC-13**: FIPS 140-2 **SC-17**: NIST 800-32; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-63 **SC-28**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-111; NIST 800-124 **SI-7**: FIPS 140-2; FIPS 180-4; FIPS 186-4; FIPS 202; NIST 800-70; NIST 800-147

5.10.1.3 Intrusion Detection Tools and Techniques	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.PT-4 **NIST**: SC-7(19), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(7), SI-4(9), SI-4(11), SI-4(12), SI-7, SI-7(1), SI-7(7)
SOC Report	IVS-07-02; SEF-02-01; SEF-05-01
Agency Responsibility	Agencies are responsible for maintaining appropriate Intrusion Detection tools within their environment.
Axon Responsibility	Axon Cloud Services employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks.
Implementation Support	**SC-7**: FIPS 199; NIST 800-41; NIST 800-77 **SI-4**: NIST 800-61; NIST 800-83; NIST 800-92; NIST 800-94; NIST 800-137 **SI-7**: FIPS 140-2; FIPS 180-4; FIPS 186-4; FIPS 202; NIST 800-70; NIST 800-147

5.10.1.5 Cloud Computing	
Control Statement	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 data centers, 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.
Control Owner	Axon
Mapping	**CSF**: ID.AM-2; ID.AM-4; ID.SC-3; PR.AC-3; PR.DS-1; PR.DS-5; PR.PT-1; DE.CM-4; DE.DP-2 **NIST**: AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-23, CP-1, CP-2(1), CP-2(3), CP-2(8), CP-6(1), CP-6(3), CP-7, CP-9, CP-10, CP-10(2), IA-1, IA-2, IR-1, IR-6, IR-8, IR-9, MA-1, MA-5, MA-5(4), MP-1, MP-2, MP-4, MP-5, MP-6, MP-7, PE-1, PE-2, PE-3, PE-18, PL-1, PL-2, PL-4, PL-4(1), PL-7, PL-8, PL-9, PS-1, PS-3, PS-7, SC-2, SC-2(1), SC-3, SC-4, SC-5, SC-5(1), SC-5(2), SC-5(3), SC-6, SC-7, SC-8, SC-12, SC-13, SC-16, SC-16(1), SC-20, SC-21, SC-22, SC-23, SC-28, SC-28(1), SC-28 (2), SC-32, SC-36, SC-38, SC-43, SI-1
SOC Report	Out of Scope; inherited from Cloud Service Provider
Agency Responsibility	Agencies are responsible for ensuring cloud resources, such as email or file sharing/storage, outside of Axon Cloud Services processing, storing or transmitting CJI or other NPI meet the requirements of this control. Appendix G.3: Cloud Computing of the CJIS Security Policy v5.9 provides additional guidance and examples to meet this control.
Axon Responsibility	Axon ensures that all CJI data and metadata in Axon Cloud Services remains within the United States, including, without limitation, all backup data, replication sites, and disaster recovery sites. Metadata derived from any CJI data is protected in the same manner as CJI data within Axon Cloud Services. Permitted use of stored CJI data and metadata is defined within agreements between agencies and Axon.

	Additional information available in **Attachment D: CJIS Appendix G.3**.
Implementation Support	**AC-17**: NIST 800-46; NIST 800-77; NIST 800-113; NIST 800-114; NIST 800-121; NISTIR 7966 **AC-23**: N/A **CP-1**: NIST 800-12; NIST 800-30; NIST 800-34; NIST 800-39; NIST 800-100 **CP-2**: NIST 800-34; NISTIR 8179 **CP-6**: NIST 800-34 **CP-7**: NIST 800-34 **CP-9**: FIPS 140-2; FIPS 186-4; NIST 800-34; NIST 800-130; NIST 800-152 **CP-10**: NIST 800-34 **IA-1**: FIPS 201; NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-100; NISTIR 7874 **IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IR-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-61; NIST 800-100 **IR-6**: NIST 800-61 **IR-8**: NIST 800-61 **IR-9**: N/A **MA-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100 **MA-5**: N/A **MP-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100 **MP-2**: FIPS 199; NIST 800-111 **MP-4**: FIPS 199; NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-111 **MP-5**: FIPS 199; NIST 800-60-1; NIST 800-60-2 **MP-6**: FIPS 199; NIST 800-60-1; NIST 800-60-2; NIST 800-88; NIST 800-124; NISTIR 8023 **MP-7**: FIPS 199; NIST 800-111 **PE-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100 **PE-2**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78 **PE-3**: FIPS 201; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-116 **PE-18**: N/A **PL-1**: NIST 800-12; NIST 800-18; NIST 800-30; NIST 800-39; NIST 800-100 **PL-2**: NIST 800-18 **PL-4**: NIST 800-18 **PL-7**: N/A **PL-8**: N/A **PL-9**: NIST 800-37 **PS-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100 **PS-3**: FIPS 199; FIPS 201; NIST 800-60-1; NIST 800-60-2; NIST 800-73; NIST 800-76; NIST 800-78 **PS-7**: NIST 800-35 **SC-2**: N/A **SC-3**: N/A **SC-4**: N/A **SC-5**: N/A **SC-6**: N/A **SC-7**: FIPS 199; NIST 800-41; NIST 800-77 **SC-8**: FIPS 140-2; FIPS 197; NIST 800-52; NIST 800-77; NIST 800-81; NIST 800-113; NIST 800-177; NISTIR 8023 **SC-12**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-63; NISTIR 7956; NISTIR 7966

	SC-13: FIPS 140-2 **SC-16**: N/A **SC-20**: FIPS 140-2; FIPS 186-4; NIST 800-81 **SC-21**: NIST 800-81 **SC-22**: NIST 800-81 **SC-23**: NIST 800-52; NIST 800-77; NIST 800-95; NIST 800-113 **SC-28**: NIST 800-56A; NIST 800-56B; NIST 800-56C; NIST 800-57-1; NIST 800-57-2; NIST 800-57-3; NIST 800-111; NIST 800-124 **SC-32**: FIPS 199 **SC-36**: N/A **SC-38**: N/A **SC-43**: NIST 800-124 **SI-1**: NIST 800-12; NIST 800-100

5.10.3 Partitioning and Virtualization	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.DS-4 **NIST**: SC-2, SC-4
Agency Responsibility	Appendix G.1: Virtualization of the CJIS Security Policy v5.9 provides additional guidance and examples to meet this control.
Axon Responsibility	Axon maintains dedicated teams to ensure Capacity Management requirements are met in a safe, secure manner.
Implementation Support	**SC-2**: N/A **SC-4**: N/A

5.10.3.1 Partitioning	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.DS-4 **NIST**: SC-2, SC-2(1), SC-3, SC-4, SC-32
SOC Report	IAM-04-01
Agency Responsibility	Appendix G.1: Virtualization of the CJIS Security Policy v5.9 provides additional guidance and examples to meet this control.
Axon Responsibility	Axon Cloud Services uses many partitioning and segmentation methods for security purposes. These include network segmentation, OS separation, firewalls, and logical access separation.
Implementation Support	**SC-2**: N/A **SC-3**: N/A **SC-4**: N/A **SC-32**: FIPS 199

5.10.3.2 Virtualization	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.DS-4 **NIST**: SC-2, SC-4
SOC Report	Out of Scope; inherited from Cloud Service Provider
Agency Responsibility	Appendix G.1: Virtualization of the CJIS Security Policy v5.9 provides additional guidance and examples to meet this control.
Axon Responsibility	Axon Cloud Services is deployed in a multi-tenant architecture, where customers leverage a shared application and underlying infrastructure. Customers are logically segmented within Axon Cloud Services and cannot access other customers' data. Application security controls and session management controls within the application prevent a customer from accessing data not associated with their account or agency. Axon leverages technologies and services provided by Infrastructure as a Service (IaaS) partners to deliver Axon Cloud Services. Axon deploys and manages virtualized servers on IaaS compute resources and leverages and manages additional IaaS services including object storage, networking, and resiliency capabilities.
Implementation Support	**SC-2**: N/A **SC-4**: N/A

5.10.4.1 Patch Management	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.DS-6; PR.IP-12 **NIST**: CM-3, CM-4, CM-4(1), RA-5, RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)
SOC Report	TVM-02-05
Agency Responsibility	Agency interaction is not typically required for patches and emergency releases of Axon Cloud Services. In the event an agency action is required, Axon will notify the Agency POC at least sixty (60) days prior to the maintenance via email.
Axon Responsibility	Axon Cloud Services ensures policies and procedures are established to ensure patches are applied within defined timeframes. Servers are patched according to the Evidence.com Patch Policy. The Axon Cloud Services routine maintenance window for US based agencies occurs on Tuesdays 2100-2200 PST. Release notes of software updates are available at least one week prior to updates occurring. Emergency maintenance outside of the scheduled maintenance window can be performed on any day of the week, but when possible will be conducted during off-peak hours and without downtime. Notification of routine maintenance is not provided in advance unless a change in the routine maintenance schedule changes.
Implementation Support	**CM-3**: NIST 800-124; NIST 800-128; NISTIR 8062 **CM-4**: NIST 800-128 **RA-5**: NIST 800-40; NIST 800-70; NIST 800-115; NIST 800-126; NISTIR 7788; NISTIR 8023 **SA-11**: NIST 800-30; NIST 800-53A; NIST 800-154 **SI-2**: FIPS 140-2; FIPS 186-4; NIST 800-40; NIST 800-128; NISTIR 7788

5.10.4.2 Malicious Code Protection	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: PR.IP-2 **NIST**: MA-3(2), PL-9, SI-3
SOC Report	IAM-06-01; IVS-07-02; TVM-02-01
Agency Responsibility	N/A
Axon Responsibility	Code change details and approvals are documented in the Axon version control system. Code changes are reviewed monthly to ensure all changes have documented approval. Development of new features, products, and major changes to Axon Cloud Services follow a Secure System Development lifecycle in alignment with industry standards, to include the OWASP Top 10 Application Security Vulnerabilities.
Implementation Support	**MA-3**: NIST 800-88 **PL-9**: NIST 800-37 **SI-3**: NIST 800-83; NIST 800-125B; NIST 800-177

5.10.4.3 Spam and Spyware Protection	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: DE.CM-4 **NIST**: PL-9, SI-8, SI-8(2)
SOC Report	TVM-01-01
Agency Responsibility	Agencies are responsible for ensuring systems accessing Axon Cloud Services and internally stored CJI have appropriate endpoint protection, properly configured network firewalls and email protection software with updated signatures.
Axon Responsibility	An advanced anti-malware solution is deployed for malware protection on Axon Cloud Services hosts and a host-based IDS/IPS solution is deployed. A web application firewall is deployed on each Axon Cloud Services web server. Additionally, vulnerability scans are performed on at least monthly basis, and penetration tests are performed at regularly.
Implementation Support	**PL-9**: NIST 800-37 **SI-8**: NIST 800-45; NIST 800-177

5.10.4.4 Security Alerts and Advisories	
Control Statement	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.
Control Owner	Axon
Mapping	**CSF**: ID.RA-2 **NIST**: SI-5, SI-5(1), SI-11
SOC Report	SEF-02-01
Agency Responsibility	Agencies are responsible for monitoring alerts and advisories for new and emerging risks which may impact their infrastructure and operations. Appendix E: Security Forums and Organizational Entities of the CJIS Security Policy provides resources to meet this control.
Axon Responsibility	Security event and incident handling practices have been implemented to ensure appropriate detection, analysis, containment, eradication, and recovery in the event of an incident. Axon employs a dedicated Security Operations team to monitor the security of Axon Cloud Services. The team is equipped to immediately respond to threats and malicious actors. Axon monitors alerts and advisories from CISA, InfraGard, MS-ISAC, and vendors for new vulnerabilities and trending threats.
Implementation Support	**SI-5**: NIST 800-40 **SI-11**: NIST 800-188

5.10.4.5 Information Input Restrictions	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-4 **NIST**: SI-10, SI-12
SOC Report	Out of Scope
Agency Responsibility	The Agency is responsible for restricting the information input to any connection to FBI CJIS services to authorized personnel only.
Axon Responsibility	N/A
Implementation Support	**SI-10**: NIST 800-167 **SI-12**: N/A

Security Policy Area 11 - Formal Audits

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division	
Control Statement	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.
Control Owner	CJIS/CSO
Mapping	**CSF**: ID.SC-4 **NIST**: CA-2, CA-7
SOC Report	Out of Scope
Agency Responsibility	Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.
Axon Responsibility	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
Implementation Support	**CA-2**: FIPS 199; NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8062 **CA-7**: NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8011; NISTIR 8062

5.11.1.2 Triennial Security Audits by the FBI CJIS Division	
Control Statement	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.
Control Owner	CJIS/CSO
Mapping	**CSF**: ID.SC-4 **NIST**: CA-2
SOC Report	Out of Scope
Agency Responsibility	Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.
Axon Responsibility	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
Implementation Support	**CA-2**: FIPS 199; NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8062

5.11.2 Audits by the CSA	
Control Statement	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.
Control Owner	CJIS/CSO
Mapping	**CSF**: ID.SC-4 **NIST**: CA-2
SOC Report	Out of Scope
Agency Responsibility	Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.
Axon Responsibility	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
Implementation Support	**CA-2**: FIPS 199; NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8062

5.11.3 Special Security Inquiries and Audits	
Control Statement	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.
Control Owner	CJIS/CSO
Mapping	**CSF**: ID.SC-4 **NIST**: CA-2(1), CA-3, CA-5, CA-6, CA-7(1), CM-3(4)
SOC Report	Out of Scope
Agency Responsibility	Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.
Axon Responsibility	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
Implementation Support	**CA-2**: FIPS 199; NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8062 **CA-3**: FIPS 199; NIST 800-47 **CA-5**: NIST 800-37 **CA-6**: NIST 800-37; NIST 800-137; NIST Supplemental Guidance on Ongoing Authorization **CA-7**: NIST 800-37; NIST 800-39; NIST 800-53A; NIST 800-115; NIST 800-122; NIST 800-137; NISTIR 8011; NISTIR 8062 **CM-3**: NIST 800-124; NIST 800-128; NISTIR 8062

CJIS Security Policy Area 12 - Personnel Security

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.IP-11 **NIST**: PS-2, PS-3, PS-3(1), PS-3(2), PS-3(3), PS-6, PS-6(2), PS-7
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.
Axon Responsibility	Axon conducts national background checks for all employees. When necessary, Axon employees that work on Axon Cloud Services are available for a fingerprint-based national record check and state-level validations.
Implementation Support	**PS-2**: N/A **PS-3**: FIPS 199; FIPS 201; NIST 800-60-1; NIST 800-60-2; NIST 800-73; NIST 800-76; NIST 800-78 **PS-6**: N/A **PS-7**: NIST 800-35

5.12.2 Personnel Termination	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.IP-11 **NIST**: PS-4
SOC Report	IAM-02-01; IAM-02-04
Agency Responsibility	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices for access management related to termination or transfer of employees. Axon will coordinate with Business Unit managers and Human Resources to identify internal employees and contractors no longer employed by Axon, customers will be updated quarterly with updated lists of CJIS approved personnel within their jurisdiction.
Implementation Support	**PS-4**: N/A

5.12.3 Personnel Transfer	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.IP-11 **NIST**: PS-5
SOC Report	IAM-02-01; IAM-02-03
Agency Responsibility	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.
Axon Responsibility	Axon maintains policies and practices for access management related to termination or transfer of employees. Axon will coordinate with Business Unit managers and Human Resources to identify internal employees and contractors whose role or responsibility no longer requires access or exposure to unencrypted CJI, customers will be updated quarterly with updated lists of CJIS approved personnel within their jurisdiction.
Implementation Support	**PS-5**: N/A

5.12.4 Personnel Sanctions	
Control Statement	The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
Control Owner	Agency
Mapping	**CSF**: PR.IP-11 **NIST**: PS-8
SOC Report	GRM-07-01
Agency Responsibility	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.
Axon Responsibility	Axon maintains a formal sanction process for employees failing to comply with established security policies and practices.
Implementation Support	**PS-8**: N/A

CJIS Security Policy Area 13 - Mobile Devices

5.13 Mobile Devices	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: DE.CM-5 **NIST**: SC-18; SI-4
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures. Axon Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence including device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) and restrict access to defined IP ranges (limit access to approved office locations). Appendix G.4 Mobile Appendix provides additional guidance and resources to assist in implementing controls in this policy area.
Axon Responsibility	N/A
Implementation Support	**SC-18**: NIST 800-28 **SI-4**: NIST 800-61; NIST 800-83; NIST 800-92; NIST 800-94; NIST 800-137

5.13.1.1 802.11 Wireless Protocols	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-5 **NIST**: AC-18, SI-4(14), SI-4(15)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address specific Wi-Fi configuration policies based on the intended use environment and data access requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**AC-18**: NIST 800-48; NIST 800-94; NIST 800-97 **SI-4**: NIST 800-61; NIST 800-83; NIST 800-92; NIST 800-94; NIST 800-137

5.13.1.2 Cellular Devices	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-3 **NIST**: AC-19, AC-19(5)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies, procedures and technical controls.
Axon Responsibility	N/A; Axon does not permit access to CJI with cellular devices, either company provided or BYOD.
Implementation Support	**AC-19**: NIST 800-114; NIST 800-124; NIST 800-164

5.13.1.2.1 Cellular Service Abroad	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-3 **NIST**: AC-19, AC-19(5)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures. Agencies should provide guidance to prevent, where possible, the transport of devices authorized to access CJI. 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.
Axon Responsibility	N/A; Axon personnel are advised to not bring company provided cellular devices when leaving the country.
Implementation Support	**AC-19**: NIST 800-114; NIST 800-124; NIST 800-164

5.13.1.2.2 Voice Transmissions Over Cellular Devices	
Control Statement	Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.
Control Owner	Agency
Mapping	**CSF**: PR.AC-3 **NIST**: AC-19, AC-19(5)
SOC Report	Out of Scope
Agency Responsibility	N/A
Axon Responsibility	N/A
Implementation Support	**AC-19**: NIST 800-114; NIST 800-124; NIST 800-164

5.13.1.3 Bluetooth	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.PT-4 **NIST**: AC-18(5)
SOC Report	Out of Scope
Agency Responsibility	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, misconfiguration 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.
Axon Responsibility	Axon devices utilizing Bluetooth technology, and connected to Axon Cloud Services, undergo security testing and validation to mitigate risk of exploitation.
Implementation Support	**AC-18**: NIST 800-48; NIST 800-94; NIST 800-97

5.13.1.4 Mobile Hotspots	
Control Statement	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 3. Ensure the hotspot SSID does not identify the device make/model or agency ownership 4. Create a wireless network password (Pre-shared key) 5. Enable the hotspot's port filtering/blocking features if present 6. 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.
Control Owner	Agency
Mapping	**CSF**: PR.PT-4 **NIST**: AC-18, AC-18(1), AC-19, IA-5, IA-5(1), SC-40, SI-4(14), SI-4(15)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures. 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 Wi-Fi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.
Axon Responsibility	N/A
Implementation Support	**AC-18**: NIST 800-48; NIST 800-94; NIST 800-97 **AC-19**: NIST 800-114; NIST 800-124; NIST 800-164 **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **SC-40**: N/A **SI-4**: NIST 800-61; NIST 800-83; NIST 800-92; NIST 800-94; NIST 800-137

5.13.2 Mobile Device Management (MDM)	
Control Statement	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: Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device. MDM with centralized administration configured and implemented to perform at least the following controls: 1. Remote locking of device 2. Remote wiping of device a. Setting and locking device configuration b. Detection of "rooted" and "jailbroken" devices c. Enforcement of folder or disk level encryption d. Application of mandatory policy settings on the device e. Detection of unauthorized configurations f. Detection of unauthorized software or applications g. Ability to determine the location of agency-controlled devices h. Prevention of unpatched devices from accessing CJI or CJI systems i. 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.
Control Owner	Agency
Mapping	**CSF**: PR.PT-4 **NIST**: AC-19, AC-19(5)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**AC-19**: NIST 800-114; NIST 800-124; NIST 800-164

5.13.3 Wireless Device Risk Mitigations	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.IP-1 **NIST**: AC-19, AC-19(5)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**AC-19**: NIST 800-114; NIST 800-124; NIST 800-164

5.13.4 System Integrity	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.IP-1 **NIST**: CM-1, CM-2, CM-2(3), CM-2(7), CM-3, CM-3(1), CM-3(2)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**CM-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-100 **CM-2**: NIST 800-124; NIST 800-128 **CM-3**: NIST 800-124; NIST 800-128; NISTIR 8062

5.13.4.1 Patching/Updates	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.IP-12 **NIST**: CM-3, CM-4, CM-4(1), RA-5, RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**CM-3**: NIST 800-124; NIST 800-128; NISTIR 8062 **CM-4**: NIST 800-128 **RA-5**: NIST 800-40; NIST 800-70; NIST 800-115; NIST 800-126; NISTIR 7788; NISTIR 8023 **SA-11**: NIST 800-30; NIST 800-53A; NIST 800-154 **SI-2**: FIPS 140-2; FIPS 186-4; NIST 800-40; NIST 800-128; NISTIR 7788

5.13.4.2 Malicious Code Protection	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.IP-2 **NIST**: MA-3(2), PL-9, SI-3
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**MA-3**: NIST 800-88 **PL-9**: NIST 800-37 **SI-3**: NIST 800-83; NIST 800-125B; NIST 800-177

5.13.4.3 Personal Firewall	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.PT-3 **NIST**: SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures. Not all mobile devices will have a functioning personal firewall or will have a limited functioning one, requiring additional configuration efforts to create the similar impact with compensating controls. An alternative is utilization of an MDM tool which limits the user's ability to downloads applications not authorized
Axon Responsibility	N/A
Implementation Support	**SC-18**: NIST 800-28

5.13.5 Incident Response	
Control Statement	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
Control Owner	Agency
Mapping	**CSF**: PR.IP-9 **NIST**: IR-1, IR-2, IR-4, IR-8
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**IR-1**: NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-61; NIST 800-83; NIST 800-100 **IR-2**: NIST 800-50 **IR-4**: NIST 800-61; NIST 800-86; NIST 800-101; NISTIR 7599 **IR-8**: NIST 800-61

5.13.6 Access Control	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-1 **NIST**: AC-5, AC-6, AC-6(5), AC-6(9), AC-19, AC-19(5)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**AC-5**: N/A **AC-6**: N/A **AC-19**: NIST 800-114; NIST 800-124; NIST 800-164

5.13.7 Identification and Authentication	
Control Statement	Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.
Control Owner	Agency
Mapping	**CSF**: PR.AC-1 **NIST**: IA-1, IA-2, IA-2(1), IA-2(2), IA-2(6), IA-2(8), IA-3, IA-5(2), MA-4, SC-37, SC-37(1)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**IA-1**: FIPS 201; NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-100; NISTIR 7874 **IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-3**: N/A **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **MA-4**: FIPS 140-2; FIPS 197; FIPS 201; NIST 800-63; NIST 800-88 **SC-37**: NIST 800-57-1; NIST 800-57-2; NIST 800-57-3

5.13.7.1 Local Device Authentication	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-1 **NIST**: IA-1, IA-2, IA-2(5)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**IA-1**: FIPS 201; NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-100; NISTIR 7874 **IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966

5.13.7.2 Advanced Authentication	
Control Statement	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.
Control Owner	Agency
Mapping	**CSF**: PR.AC-7 **NIST**: IA-2(1), IA-2(2), IA-2(6), IA-2(11), IA-2(13), IA-3(1), IA-5(2), MA-4, SC-37, SC-37(1)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**IA-1**: FIPS 201; NIST 800-12; NIST 800-30; NIST 800-39; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-100; NISTIR 7874 **IA-2**: FIPS 140-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NIST 800-79; NIST 800-156; NIST 800-166; NISTIR 7539; NISTIR 7676; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 7874; NISTIR 7966 **IA-3**: N/A **IA-5**: FIPS 140-2; FIPS 180-2; FIPS 201; FIPS 202; NIST 800-63; NIST 800-73; NIST 800-76; NIST 800-78; NISTIR 7539; NISTIR 7817; NISTIR 7849; NISTIR 7870; NISTIR 8040 **MA-4**: FIPS 140-2; FIPS 197; FIPS 201; NIST 800-63; NIST 800-88 **SC-37**: NIST 800-57-1; NIST 800-57-2; NIST 800-57-3

5.13.7.2.1 Compensating Controls	
Control Statement	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
Control Owner	Agency
Mapping	**CSF**: PR.AC-7 **NIST**: AC-19, IA-3, IA-3(4), PE-18, PE-20, PE-23
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**AC-19**: NIST 800-114; NIST 800-124; NIST 800-164 **IA-3**: N/A **PE-18**: N/A **PE-20**: N/A **PE-23**: N/A

5.13.7.3 Device Certificates	
Control Statement	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
Control Owner	Agency
Mapping	**CSF**: PR.AC-6 **NIST**: AC-19, IA-3, IA-3(4)
SOC Report	Out of Scope
Agency Responsibility	Agencies must address this requirement through appropriate policies and procedures.
Axon Responsibility	N/A
Implementation Support	**AC-19**: NIST 800-114; NIST 800-124; NIST 800-164 **IA-3**: N/A

Attachments

Attachment A: Certificate of Liability Insurance

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY) 10/05/2020

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
Aon Risk Insurance Services West, Inc. Phoenix AZ Office 2555 East Camelback Rd. Suite 700 Phoenix AZ 85016 USA	PHONE (A/C. No. Ext): (866) 283-7122	FAX (A/C. No.): (800) 363-0105
	E-MAIL ADDRESS:	

INSURED	INSURER(S) AFFORDING COVERAGE	NAIC #
Axon Enterprise, Inc.; MediaSolv Solutions Corporation; Vievu, LLC 17800 N. 85th Street Scottsdale AZ 85255 USA	INSURER A: Endurance American Specialty Ins Co.	41718
	INSURER B:	
	INSURER C:	
	INSURER D:	
	INSURER E:	
	INSURER F:	

COVERAGES **CERTIFICATE NUMBER:** 570084424618 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. **Limits shown are as requested**

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	COMMERCIAL GENERAL LIABILITY CLAIMS-MADE OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: POLICY PRO-JECT LOC OTHER:						EACH OCCURRENCE	
							DAMAGE TO RENTED PREMISES (Ea occurrence)	
							MED EXP (Any one person)	
							PERSONAL & ADV INJURY	
							GENERAL AGGREGATE	
							PRODUCTS - COMP/OP AGG	
	AUTOMOBILE LIABILITY ANY AUTO OWNED AUTOS ONLY HIRED AUTOS ONLY SCHEDULED AUTOS NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident)	
							BODILY INJURY (Per person)	
							BODILY INJURY (Per accident)	
							PROPERTY DAMAGE (Per accident)	
	UMBRELLA LIAB OCCUR EXCESS LIAB CLAIMS-MADE DED RETENTION						EACH OCCURRENCE	
							AGGREGATE	
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y / N N / A					PER STATUTE OTH-ER	
							E.L. EACH ACCIDENT	
							E.L. DISEASE-EA EMPLOYEE	
							E.L. DISEASE-POLICY LIMIT	
A	E&O-Technology			PRO10013803302 Cyber/Tech E&O ClmsMade SIR applies per policy terms & conditions	09/30/2020	09/30/2021	Ea. Claim Limit Ea. Claim SIR Max. Aggregate Limi	$5,000,000 $100,000 $5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Proof of Insurance.

CERTIFICATE HOLDER

Axon Enterprise, Inc.
17800 N. 85th Street
Scottsdale AZ 85255 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

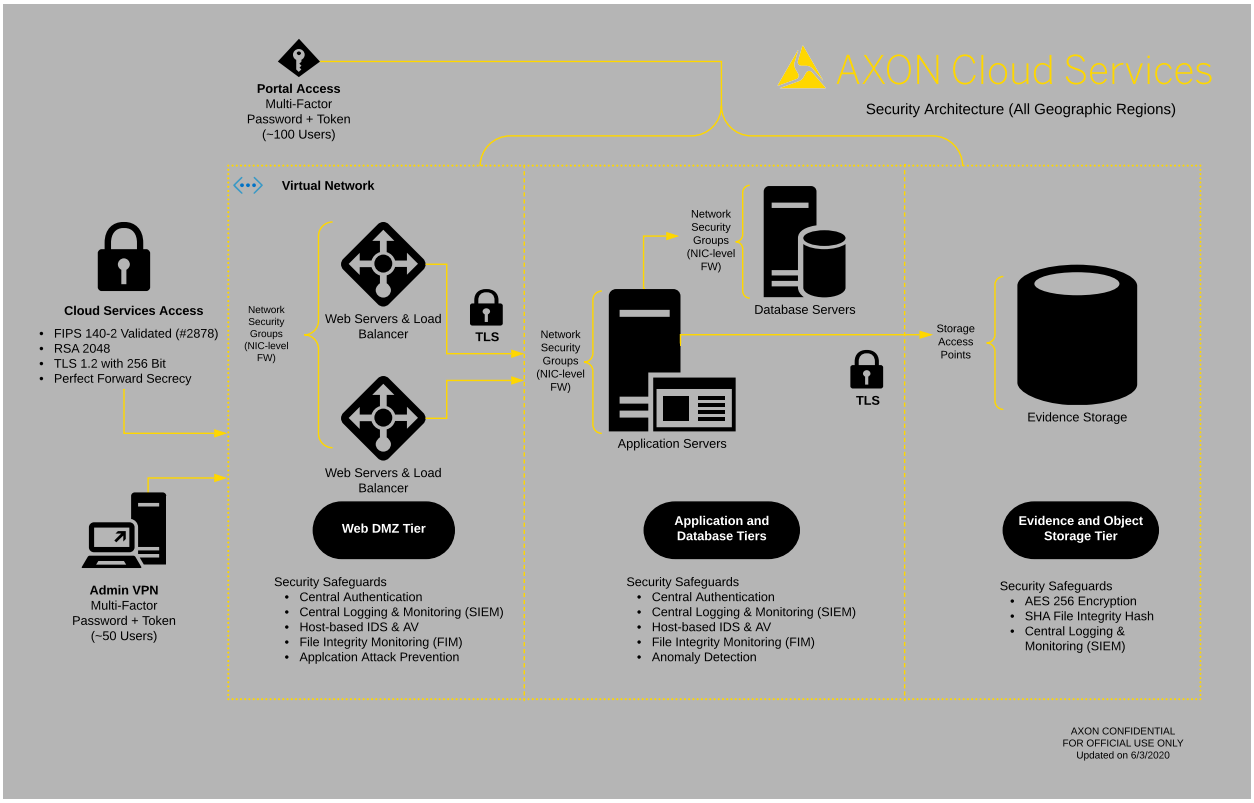
Aon Risk Insurance Services West, Inc.

Holder Identifier :

Certificate No : 570084424618

ACORD 25 (2016/03) The ACORD name and logo are registered marks of ACORD

Attachment B: Network and Security Architecture Diagram



Attachment C: FIPS 140-2 Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

April 2017

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions. Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States
Signature: Michael Cooper
Dated: 5/1/2017
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature:
Dated: MAY 0 2 2017
Director, Architecture and Technology Assurance
Communications Security Establishment

Certificate Number	Validation / Posting Date			Version Information
2873	04/04/2017	VMAX 6 Gb/s SAS I/O Module with Encryption	Dell EMC	Hardware Version: 303-161-101B-05; Firmware Version: 2.13.46.00
2874	04/05/2017	Barracuda KTINA FIPS Crypto Module	Barracuda Networks	Software Version: 7.1
2875	04/05/2017	Forcepoint C Cryptographic Module	Forcepoint	Software Version: 2.0.2, 2.0.5 or 2.0.10
2876	04/06/2017	KMF/Wave/Traffic CryptR	Motorola Solutions, Inc.	Hardware Version: P/N CLN6566A; Firmware Version: R02.01.05
2877	04/06/2017	WatchGuard Firebox T10[1], T10-W[2], T30[3], T30-W[4], T50[5], T50-W[6]	WatchGuard Technologies, Inc.	Hardware Version: DS1AE3 [1]; DS3AE3 [2]; BS3AE5 [3]; BS3AE0W [4]; BS5AE7 [5], BS5AE7W [6], FIPS Kit P/N: WG85BE; Firmware Version: Fireware OS v11.11.2
2878	04/06/2017	Axon Cryptographic Module	Axon Enterprise, Inc	Software Version: 2.1
2879	04/11/2017	Barco ICMP	Barco n.v.	Hardware Version: R7681272 02; Firmware Version: 1.3.0.157358
2880	04/11/2017	HGST Ultrastar C10K1800 TCG Enterprise HDDs	HGST, a Western Digital company	Hardware Version: HUC101818CS4205 (2), HUC101818CS4206 (3), HUC101812CS4205 (2), HUC101812CS4206 (3), HUC101890CS4205 (2), HUC101890CS4206 (3), HUC101845CS4205 (2), HUC101845CS4206 (3), HUC101812CSS205 (2), HUC101812CSS206 (3), HUC101890CSS205 (2), HUC101890CSS206 (3), HUC101860CSS205 (2), HUC101860CSS206 (3), HUC101830CSS205 (2), HUC101830CSS206 (3); Firmware Version: RAA2
2881	04/13/2017	SPYCOS 3.0 microSDHC(TM) TrustedFlash Module	SPYRUS, Inc.	Hardware Version: 851-315013F (16GB) and 851-315014F (32GB); Firmware Version: 1.0
2883	04/18/2017	HGST Ultrastar C15K600 TCG Enterprise HDDs	HGST, a Western Digital company	Hardware Version: HUC156060CS4205 (2), HUC156045CS4205 (2), HUC156030CS4205 (2), HUC156060CS5205 (2), HUC156045CS5205 (2), HUC156030CS5205 (2); Firmware Version: RAA2
2884	04/19/2017	Mercury Systems ASURRE-Stor™ SSD	Mercury Systems, Inc.	Hardware Version: P/Ns ASD256AM2R-0yzIF, 3.0; ASD512AM2R-0yzIF, 3.0; ADR256AM2R-0yzIF, 3.0; ADR512AM2R-0yzIF, 3.0 (as described in Security Policy, Table 4); Firmware Version: 1.5.0
2885	04/19/2017	Dell SMA Series v11.4 EX6000, EX7000, EX8000, SMA 6200, SMA 7200	Dell Software, Inc.	Hardware Version: P/Ns 101-500210-78 Rev A, 101-500188-78 Rev A, 101-500352-62 Rev A, 101-500390-61 Rev B, 101-500388-61 Rev B; Firmware Version: 11.4.0-512
2886	04/20/2017	Seagate Secure(R) TCG Enterprise SSC Self-Encrypting Drive	Seagate Technology LLC	Hardware Version: ST10000NM0176 [1] and ST10000NM0188 [2]; Firmware Version: SF02 [1] and NF02 [2]
2887	04/21/2017	FortiGate-VM Virtual Appliance	Fortinet, Inc.	Software Version: FortiGate-VM64 v5.2.7,build0718,160328
2888	04/24/2017	Ubuntu OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 1.0

Attachment D: Axon CJIS Security Addendum

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

Jenner Holden _____ _____
Printed Name/Signature of Contractor Representative Date

AXON Enterprise, Inc. CISO
Organization and Title of Contractor Representative

Attachment E: CJIS Appendix G.3 Cloud Computing

Appendix G.3 Questions	Axon Cloud Services Policies, Practices, and Standards
Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)	Axon maintains policies and practices for Axon Cloud Services that limit remote access to only required individuals, via managed VPN connections requiring at least 2-factor authentication.
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)	Axon Cloud Services require at least 2-factor authentication for all system administration access. 2-factor authentication is available for individual customer accounts.
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)	Axon regularly reviews the specific security practices and audit results documented by Infrastructure as a Service (IaaS) partners to ensure they meet the relevant portions of the CJIS Security Policy.
Are the encryption requirements being met? (5.10.1.2 Encryption) o 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. o Is the data encrypted while at rest and in transit?	Axon securely provides, stores, and maintains encryption keys. Data transmitted and stored in Axon Cloud Services is encrypted with 128 bits or stronger. FIPS 140-2 approved encryption ciphers (or stronger) are used, including AES 256, and RSA 2048. Axon maintains policies and practices for Axon Cloud Services for encryption key and certificate management.
What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response) o Will the cloud subscriber be notified of any incident? o If CJI is compromised, what are the notification and response procedures?	Axon maintains comprehensive security incident response plans for Axon Cloud Services including reporting to appropriate parties.
Is the cloud service provider a private contractor/vendor? o 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)	Axon acknowledges and abides by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is included by reference in the Axon MSPA which contractually commits Axon to the CJIS Security Policy requirements. CJIS Security Addendum Certification pages are maintained for each authorized Axon employee and are available to customers. Axon maintains policies and practices for ensuring all Axon Cloud Services personnel are trustworthy and competent to handle sensitive data and systems. Authorized Axon personnel are available for state of residence and national fingerprint-based record checks at either the state or local level.
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)	Axon adheres to the audit requirements of the FBI CJIS Security Policy.
How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability) o Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request? o What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.9 Policy Area 8: Media Protection)	Axon Cloud Services systems are configured to log all required events from Policy Area 4, and more, to a central logging system.

Attachment F – Control Crosswalks

ATTACHMENT F.1 NIST 800-53 v5 to CJIS v5.9.1

Control ID	Control Name	Enhancement Controls	CJIS Control
AC-1	Access Control Policy and Procedures		5.5 Access Control
AC-2	Account Management	AC-2 (1) (4) (7)	5.5.1 Account Management 5.5.2 Access Enforcement 5.5.2.1 Least Privilege 5.5.2.2 System Access Control 5.5.2.3 Access Control Criteria 5.5.2.4 Access Control Mechanisms
AC-3	Access Enforcement	AC-3 (3) (4)	5.5.2 Access Enforcement
AC-4	Information Flow Enforcement		5.10.1 Information Flow Enforcement
AC-5	Separation of Duties		5.5.1 Account Management 5.5.2 Access Enforcement 5.5.2.1 Least Privilege 5.5.2.2 System Access Control 5.5.2.3 Access Control Criteria 5.5.2.4 Access Control Mechanisms 5.13.6 Access Control
AC-6	Least Privilege	AC-6 (1) (2) (5) (9)	5.5.2 Access Enforcement 5.5.2.1 Least Privilege 5.5.2.2 System Access Control 5.5.2.3 Access Control Criteria 5.5.2.4 Access Control Mechanisms 5.13.6 Access Control
AC-7	Unsuccessful Logon Attempts		5.5.3 Unsuccessful Login Attempts
AC-8	System Use Notification		5.5.4 System Use Notification
AC-9	Previous Logon (Access) Notification		5.4.1 Auditable Events and Content (Information Systems) 5.4.1.1 Events
AC-10	Concurrent Session Control		5.5.2.1 Least Privilege 5.5.2.2 System Access Control 5.5.2.3 Access Control Criteria 5.5.2.4 Access Control Mechanisms
AC-11	Device Lock	AC-11 (1)	5.5.4 System Use Notification 5.5.5 Session Lock
AC-12	Session Termination	AC-12 (1)	5.5.2 Access Enforcement
AC-17	Remote Access	AC-17 (1) (2) (3) (4) (6)	5.5.6 Remote Access 5.5.6.1 Personally Owned Information Systems 5.5.6.2 Publicly Accessible Computers 5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.10.1.2.2 Encryption for CJI at Rest 5.10.1.5 Cloud Computing
AC-18	Wireless Access	AC-18 (1) (5)	5.13.1.1 802.11 Wireless Protocols 5.13.1.3 Bluetooth 5.13.1.4 Mobile Hotspots
AC-19	Access Control for Mobile Devices	AC-19 (5)	5.13.1.2 Cellular Devices 5.13.1.2.1 Cellular Service Abroad 5.13.1.2.2 Voice Transmissions Over Cellular Devices 5.13.1.4 Mobile Hotspots 5.13.2 Mobile Device Management (MDM) 5.13.3 Wireless Device Risk Mitigations 5.13.6 Access Control 5.13.7.2.1 Compensating Controls 5.13.7.3 Device Certificates
AC-20	Use of External Systems	AC-20 (1) (2)	5.8.1 Media Storage and Access 5.10.1 Information Flow Enforcement 5.10.1.1 Boundary Protection

AC-21	Information Sharing		5.1.1 Information Exchange 5.1.1.1 Information Handling 5.1.1.2 State and Federal Agency User Agreements 5.1.1.3 Criminal Justice Agency User Agreements 5.1.1.4 Interagency and Management Control Agreements 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 5.1.1.6 Agency User Agreements
AC-22	Publicly Accessible Content		5.5.4 System Use Notification 5.5.6.2 Publicly Accessible Computers
AC-23	Data Mining Protection		5.10.1.5 Cloud Computing
AT-1	Awareness and Training Policy and Procedures		5.2 Basic Security Awareness Training
AT-2	Awareness Training	AT-2 (2)	5.2.1.1 Level One Security Awareness Training 5.2.1.2 Level Two Security Awareness Training 5.2.1.3 Level Three Security Awareness Training
AT-3	Role-Based Training		5.2.1.1 Level One Security Awareness Training 5.2.1.2 Level Two Security Awareness Training 5.2.1.3 Level Three Security Awareness Training 5.2.1.4 Level Four Security Awareness Training
AT-4	Training Records		5.2.3 Security Training Records
AU-1	Audit and Accountability Policy and Procedures		5.4 Auditing and Accountability
AU-2	Audit Events		5.4.1 Auditable Events and Content (Information Systems) 5.4.1.1 Events
AU-3	Content of Audit Records	AU-3 (1)	5.4.1 Auditable Events and Content (Information Systems)
AU-4	Audit Storage Capacity		5.4.6 Audit Record Retention 5.4.7 Logging NCIC and III Transactions
AU-5	Response to Audit Processing Failures	AU-5 (1) (2)	5.4.2 Response to Audit Processing Failures 5.4.6 Audit Record Retention
AU-6	Audit Review, Analysis, and Reporting	AU-6 (1) (3)	5.4.1 Auditable Events and Content (Information Systems) 5.4.3 Audit Monitoring, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation		5.4.3 Audit Monitoring, Analysis, and Reporting
AU-8	Time Stamps		5.4.4 Time Stamps
AU-9	Protection of Audit Information		5.4.5 Protection of Audit Information 5.4.6 Audit Record Retention
AU-11	Audit Record Retention		5.4.6 Audit Record Retention 5.4.7 Logging NCIC and III Transactions
AU-12	Audit Generation		5.4.1 Auditable Events and Content (Information Systems) 5.4.1.1 Events 5.4.1.1.1 Content
CA-2	Assessments	CA-2 (1)	5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division 5.11.1.2 Triennial Security Audits by the FBI CJIS Division 5.11.2 Audits by the CSA 5.11.3 Special Security Inquiries and Audits

CA-3	System Interconnections		5.1.1 Information Exchange 5.1.1.2 State and Federal Agency User Agreements 5.1.1.3 Criminal Justice Agency User Agreements 5.1.1.4 Interagency and Management Control Agreements 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 5.1.1.6 Agency User Agreements 5.7.1.2 Network Diagram 5.10.1 Information Flow Enforcement 5.11.3 Special Security Inquiries and Audits
CA-5	Plan of Action and Milestones		5.11.3 Special Security Inquiries and Audits
CA-6	Authorization		5.11.3 Special Security Inquiries and Audits
CA-7	Continuous Monitoring	CA-7 (1)	5.4.1 Auditable Events and Content (Information Systems) 5.4.1.1 Events 5.4.3 Audit Monitoring, Analysis, and Reporting 5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division 5.11.3 Special Security Inquiries and Audits
CA-9	Internal System Connections		5.7.1.2 Network Diagram 5.10.1 Information Flow Enforcement
CM-2	Baseline Configuration		5.7.1.1 Least Functionality 5.7.2 Security of Configuration Documentation
CM-3	Configuration Change Control	CM-3 (2) (4) (7)	5.7.1 Access Restrictions for Changes 5.7.1.1 Least Functionality 5.7.2 Security of Configuration Documentation 5.10.4.1 Patch Management 5.11.3 Special Security Inquiries and Audits 5.13.4.1 Patching/Updates
CM-4	Security and Privacy Impact Analyses	CM-4 (1) (2)	5.7.1 Access Restrictions for Changes 5.10.4.1 Patch Management 5.13.4.1 Patching/Updates
CM-5	Access Restrictions for Change	CM-5 (1) (5) (6)	5.7.1 Access Restrictions for Changes 5.7.2 Security of Configuration Documentation
CM-6	Configuration Settings		5.7.1 Access Restrictions for Changes 5.7.1.1 Least Functionality
CM-7	Least Functionality	CM-7 (1) (2) (3) (4) (5)	5.7.1.1 Least Functionality
CM-8	System Component Inventory	CM-8 (1) (3)	5.7.1.1 Least Functionality 5.7.2 Security of Configuration Documentation
CM-9	Configuration Management Plan		5.1.1.1 Information Handling 5.7.1 Access Restrictions for Changes 5.7.2 Security of Configuration Documentation
CM-10	Software Usage Restrictions		5.2.1.4 Level Four Security Awareness Training 5.7.1.1 Least Functionality
CM-11	User-Installed Software		5.7.1.1 Least Functionality
CP-1	Contingency Planning Policy and Procedures		5.10.1.5 Cloud Computing
CP-2	Contingency Plan	CP-2 (1) (3) (8)	5.10.1.5 Cloud Computing
CP-6	Alternate Storage Site	CP-6 (1) (3)	5.1.1.1 Information Handling 5.8.1 Media Storage and Access 5.10.1.5 Cloud Computing
CP-7	Alternate Processing Site		5.1.1.1 Information Handling 5.8.1 Media Storage and Access 5.10.1.5 Cloud Computing
CP-9	System Backup		5.10.1.5 Cloud Computing
CP-10	System Recovery and Reconstitution		5.10.1.5 Cloud Computing
IA-1	Identification and Authentication Policy and Procedures		5.6 Identification and Authentication 5.6.1 Identification Policy and Procedures 5.6.2 Authentication Policy and Procedures 5.10.1.5 Cloud Computing 5.13.7 Identification and Authentication 5.13.7.1 Local Device Authentication

IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (2) (5) (6) (8) (9) (11) (12) (13)	5.6.1 Identification Policy and Procedures 5.6.2 Authentication Policy and Procedures 5.6.2.1.3 One-time Passwords (OTP) 5.6.2.2 Advanced Authentication 5.6.2.2.1 Advanced Authentication Policy and Rationale 5.6.4 Assertions 5.10.1.2.3 Public Key Infrastructure (PKI) Technology 5.10.1.5 Cloud Computing 5.13.7 Identification and Authentication 5.13.7.1 Local Device Authentication 5.13.7.2 Advanced Authentication
IA-3	Device Identification and Authentication	IA-3 (1) (4)	5.6.2 Authentication Policy and Procedures 5.6.2.2 Advanced Authentication 5.6.2.2.1 Advanced Authentication Policy and Rationale 5.13.7 Identification and Authentication 5.13.7.2 Advanced Authentication 5.13.7.2.1 Compensating Controls 5.13.7.3 Device Certificates
IA-4	Identifier Management	IA-4 (4)	5.6.3 Identifier and Authenticator Management
IA-5	Authenticator Management	IA-5 (1) (2) (5) (6) (7) (8) (10)	5.5.3 Unsuccessful Login Attempts 5.6.2.1 Standard Authenticators 5.6.2.1.1 Password 5.6.2.1.1.1 Basic Password Standards 5.6.2.1.1.2 Advanced Password Standards 5.6.2.1.2 Personal Identification Number (PIN) 5.6.2.1.3 One-time Passwords (OTP) 5.6.2.2 Advanced Authentication 5.6.2.2.1 Advanced Authentication Policy and Rationale 5.6.3 Identifier and Authenticator Management 5.6.3.2 Authenticator Management 5.10.1 Information Flow Enforcement 5.10.1.2.3 Public Key Infrastructure (PKI) Technology 5.13.1.4 Mobile Hotspots 5.13.7 Identification and Authentication 5.13.7.2 Advanced Authentication
IA-6	Authenticator Feedback		5.6.2.1 Standard Authenticators
IA-7	Cryptographic Module Authentication		5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.10.1.2.2 Encryption for CJI at Rest 5.10.1.2.3 Public Key Infrastructure (PKI) Technology
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (5)	5.6.3 Identifier and Authenticator Management 5.6.4 Assertions 5.10.1.2.3 Public Key Infrastructure (PKI) Technology
IA-12	Identity Proofing	IA-12 (1) (4)	5.6.2.1.3 One-time Passwords (OTP) 5.6.3 Identifier and Authenticator Management
IR-1	Incident Response Policy and Procedures		5.3 Incident Response 5.3.2 Management of Security Incidents 5.10.1.5 Cloud Computing 5.13.5 Incident Response
IR-2	Incident Response Training		5.3.3 Incident Response Training 5.13.5 Incident Response
IR-3	Incident Response Testing		5.3.3 Incident Response Training
IR-4	Incident Handling	IR-4 (1) (3) (4)	5.3.1 Reporting Security Events 5.3.2.1 Incident Handling 5.3.2.2 Collection of Evidence 5.13.5 Incident Response

IR-5	Incident Monitoring		5.3.4 Incident Monitoring
IR-6	Incident Reporting	IR-6 (1) (2)	5.3.1 Reporting Security Events 5.10.1.5 Cloud Computing
IR-7	Incident Response Assistance	IR-7 (1) (2)	5.3.1 Reporting Security Events
IR-8	Incident Response Plan		5.1.1.1 Information Handling 5.3.1 Reporting Security Events 5.3.2 Management of Security Incidents 5.3.2.1 Incident Handling 5.3.2.2 Collection of Evidence 5.5.1 Account Management 5.10.1.5 Cloud Computing 5.13.5 Incident Response
IR-9	Information Spillage Response		5.10.1.5 Cloud Computing
MA-1	System Maintenance Policy and Procedures		5.10.1.5 Cloud Computing
MA-2	Controlled Maintenance		5.7.1 Access Restrictions for Changes 5.8.3 Digital Media Sanitization and Disposal
MA-3	Maintenance Tools	MA-3 (2) (3)	5.8.1 Media Storage and Access 5.10.4.2 Malicious Code Protection 5.13.4.2 Malicious Code Protection
MA-4	Nonlocal Maintenance	MA-4 (6) (7)	5.6.2.2 Advanced Authentication 5.6.2.2.1 Advanced Authentication Policy and Rationale 5.9.1.2 Physical Access Authorizations 5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.13.7 Identification and Authentication 5.13.7.2 Advanced Authentication
MA-5	Maintenance Personnel		5.7.1 Access Restrictions for Changes 5.9.1.2 Physical Access Authorizations 5.10.1.5 Cloud Computing
MP-1	Media Protection Policy and Procedures		5.10.1.5 Cloud Computing
MP-2	Media Access		5.10.1.5 Cloud Computing
MP-3	Media Marking		
MP-4	Media Storage		5.10.1.5 Cloud Computing
MP-5	Media Transport		5.10.1.5 Cloud Computing
MP-6	Media Sanitization		5.10.1.5 Cloud Computing
MP-7	Media Use		5.10.1.5 Cloud Computing
PE-1	Physical and Environmental Protection Policy and Procedures		5.9 Physical Protection 5.9.1 Physically Secure Location 5.9.1.1 Security Perimeter 5.10.1.5 Cloud Computing
PE-2	Physical Access Authorizations	PE-2 (1) (3)	5.9.1.2 Physical Access Authorizations 5.9.1.7 Visitor Control 5.9.2 Controlled Area 5.10.1.5 Cloud Computing
PE-3	Physical Access Control	PE-3 (2) (3)	5.9.1.3 Physical Access Control 5.9.1.6 Monitoring Physical Access 5.9.1.7 Visitor Control 5.10.1.1 Boundary Protection 5.10.1.5 Cloud Computing
PE-4	Access Control for Transmission		5.9.1.4 Access Control for Transmission Medium
PE-5	Access Control for Output Devices		5.9.1.5 Access Control for Display Medium 5.9.1.6 Monitoring Physical Access 5.9.2 Controlled Area
PE-6	Monitoring Physical Access	PE-6 (1)	5.9.1.6 Monitoring Physical Access
PE-8	Visitor Access Records		5.9.1.8 Delivery and Removal
PE-17	Alternate Work Site		5.3.1 Reporting Security Events
PE-18	Location of System Components		5.10.1.5 Cloud Computing 5.13.7.2.1 Compensating Controls
PE-20	Asset Monitoring and Tracking		5.13.7.2.1 Compensating Controls
PE-23	Facility Location		5.13.7.2.1 Compensating Controls
PL-1	Planning Policy and Procedures		5.10.1.5 Cloud Computing

PL-2	System Security and Privacy Plans		5.1.1.1 Information Handling 5.10.1.5 Cloud Computing
PL-4	Rules of Behavior	PL-4 (1)	5.2 Basic Security Awareness Training 5.2.1.2 Level Two Security Awareness Training 5.2.1.3 Level Three Security Awareness Training 5.2.3 Security Training Records 5.10.1.5 Cloud Computing
PL-7	Concept of Operations		5.10.1.5 Cloud Computing
PL-8	Security and Privacy Architectures		5.10.1.5 Cloud Computing
PL-9	Central Management		5.10.1.5 Cloud Computing 5.10.4.2 Malicious Code Protection 5.10.4.3 Spam and Spyware Protection 5.13.4.2 Malicious Code Protection
PM-1	Information Security Program Plan		5.1.1.1 Information Handling
PS-1	Personnel Security Policy and Procedures		5.10.1.5 Cloud Computing
PS-2	Position Risk Designation		5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI
PS-3	Personnel Screening	PS-3 (1) (2) (3)	5.1.3 Secondary Dissemination 5.1.4 Secondary Dissemination of Non-CHRI CJI 5.10.1.5 Cloud Computing 5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI
PS-4	Personnel Termination		5.12.2 Personnel Termination
PS-5	Personnel Transfer		5.12.3 Personnel Transfer
PS-6	Access Agreements	PS-6 (2)	5.1.3 Secondary Dissemination 5.1.4 Secondary Dissemination of Non-CHRI CJI 5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI
PS-7	External Personnel Security		5.1.3 Secondary Dissemination 5.1.4 Secondary Dissemination of Non-CHRI CJI 5.10.1.5 Cloud Computing 5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI
PS-8	Personnel Sanctions		5.12.4 Personnel Sanctions
RA-3	Risk Assessment		5.1.2 Monitoring, Review, and Delivery of Services 5.1.2.1 Managing Changes to Service Providers
RA-5	Vulnerability Scanning	RA-5 (2) (3) (5)	5.5.2.1 Least Privilege 5.5.2.2 System Access Control 5.5.2.3 Access Control Criteria 5.5.2.4 Access Control Mechanisms 5.10.4.1 Patch Management 5.13.4.1 Patching/Updates
SA-2	Allocation of Resources		5.1.1 Information Exchange 5.1.1.2 State and Federal Agency User Agreements 5.1.1.3 Criminal Justice Agency User Agreements 5.1.1.4 Interagency and Management Control Agreements 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 5.1.1.6 Agency User Agreements

SA-4	Acquisition Process	SA-4 (1) (9)	5.1.1 Information Exchange 5.1.1.2 State and Federal Agency User Agreements 5.1.1.3 Criminal Justice Agency User Agreements 5.1.1.4 Interagency and Management Control Agreements 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 5.1.1.6 Agency User Agreements 5.7.1.1 Least Functionality
SA-5	System Documentation		5.7.2 Security of Configuration Documentation
SA-9	External System Services	SA-9 (1) (2)	5.1.2 Monitoring, Review, and Delivery of Services 5.7.1.1 Least Functionality
SA-10	Developer Configuration Management		5.7.1 Access Restrictions for Changes
SA-11	Developer Security Testing and Evaluation	SA-11 (1)	5.10.4.1 Patch Management 5.13.4.1 Patching/Updates
SC-2	Application Partitioning	SC-2 (1)	5.10.1.5 Cloud Computing 5.10.3 Partitioning and Virtualization 5.10.3.1 Partitioning 5.10.3.2 Virtualization
SC-3	Security Function Isolation		5.10.1.5 Cloud Computing 5.10.3.1 Partitioning
SC-4	Information in Shared Systems Resources		5.10.1.5 Cloud Computing 5.10.3 Partitioning and Virtualization 5.10.3.1 Partitioning 5.10.3.2 Virtualization
SC-5	Denial of Service Protection	SC-5 (1) (2) (3)	5.10.1.1 Boundary Protection 5.10.1.5 Cloud Computing
SC-6	Resource Availability		5.10.1.5 Cloud Computing
SC-7	Boundary Protection	SC-7 (3) (4) (5) (7) (8) (11) (12) (13) (14) (18) (19) (25)	5.7.1.2 Network Diagram 5.10.1 Information Flow Enforcement 5.10.1.1 Boundary Protection 5.10.1.3 Intrusion Detection Tools and Techniques 5.10.1.5 Cloud Computing
SC-8	Transmission Confidentiality and Integrity	SC-8 (1) (2)	5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.10.1.5 Cloud Computing
SC-10	Network Disconnect		5.10.1 Information Flow Enforcement
SC-11	Trusted Path		5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit
SC-12	Cryptographic Key Establishment and Management	SC-12 (1) (2) (3)	5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.10.1.2.2 Encryption for CJI at Rest 5.10.1.2.3 Public Key Infrastructure (PKI) Technology 5.10.1.5 Cloud Computing
SC-13	Cryptographic Protection		5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.10.1.2.2 Encryption for CJI at Rest 5.10.1.2.3 Public Key Infrastructure (PKI) Technology 5.10.1.5 Cloud Computing
SC-15	Collaborative Computing Devices and Applications	SC-15 (1)	5.10.1 Information Flow Enforcement
SC-16	Transmission of Security and Privacy Attributes	SC-16 (1)	5.10.1.5 Cloud Computing
SC-17	Public Key Infrastructure Certificates		5.10.1.2 Encryption 5.10.1.2.3 Public Key Infrastructure (PKI) Technology
SC-18	Mobile Code	SC-18 (1) (2) (3) (4)	5.13 Mobile Devices 5.13.4.3 Personal Firewall

SC-20	Secure Name /Address Resolution Service (Authoritative Source)		5.10.1.5 Cloud Computing
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)		5.10.1.5 Cloud Computing
SC-22	Architecture and Provisioning for Name/Address Resolution Service		5.10.1.5 Cloud Computing
SC-23	Session Authenticity	AC-23 (1) (3)	5.5.2 Access Enforcement 5.10.1.5 Cloud Computing
SC-24	Fail in Known State		5.10.1.1 Boundary Protection
SC-28	Protection of Information at Rest	SC-28 (1) (2)	5.8.2.1 Digital Media during Transport 5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.10.1.2.2 Encryption for CJI at Rest 5.10.1.2.3 Public Key Infrastructure (PKI) Technology 5.10.1.5 Cloud Computing
SC-32	System Partitioning		5.10.1.5 Cloud Computing 5.10.3.1 Partitioning
SC-36	Distributed Processing and Storage		5.10.1.5 Cloud Computing
SC-37	Out-of-Band Channels	SC-37 (1)	5.6.2.1.3 One-time Passwords (OTP) 5.6.2.2 Advanced Authentication 5.13.7 Identification and Authentication 5.13.7.2 Advanced Authentication
SC-38	Operations Security		5.10.1.5 Cloud Computing
SC-40	Wireless Link Protection		5.13.1.4 Mobile Hotspots
SC-43	Usage Restrictions		5.10.1.5 Cloud Computing
SC-45	System Time Synchronization	SC-45 (1)	5.4.4 Time Stamps
SI-1	System and Information Integrity Policy and Procedures		5.10.1.5 Cloud Computing
SI-2	Flaw Remediation	SI-2 (2) (3)	5.10.4.1 Patch Management 5.13.4.1 Patching/Updates
SI-3	Malicious Code Protection		5.10.4.2 Malicious Code Protection 5.13.4.2 Malicious Code Protection
SI-4	System Monitoring	SI-4 (1) (2) (4) (5) (7) (9) (11) (12) (14) (15)	5.4.3 Audit Monitoring, Analysis, and Reporting 5.10.1.3 Intrusion Detection Tools and Techniques 5.13 Mobile Devices 5.13.1.1 802.11 Wireless Protocols 5.13.1.4 Mobile Hotspots
SI-5	Security Alerts, Advisories, and Directives	SI-5 (1)	5.10.4.4 Security Alerts and Advisories
SI-7	Software, Firmware, and Information Integrity	SI-7 (1) (6) (7)	5.10.1.2 Encryption 5.10.1.2.1 Encryption for CJI in Transit 5.10.1.2.2 Encryption for CJI at Rest 5.10.1.2.3 Public Key Infrastructure (PKI) Technology 5.10.1.3 Intrusion Detection Tools and Techniques
SI-8	Spam Protection	SI-8 (2)	5.10.4.3 Spam and Spyware Protection
SI-10	Information Input Validation		5.10.4.5 Information Input Restrictions
SI-11	Error Handling		5.10.4.4 Security Alerts and Advisories
SI-12	Information Management and Retention		5.10.4.5 Information Input Restrictions
SR-6	Supplier Assessments and Reviews		5.1.1 Information Exchange 5.1.1.2 State and Federal Agency User Agreements 5.1.1.3 Criminal Justice Agency User Agreements 5.1.1.4 Interagency and Management Control Agreements 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 5.1.1.6 Agency User Agreements

ATTACHMENT F.2 NIST CSF v1.1 to CJIS v5.9.1

Subcategory	CJIS 5.9
ID.AM-1: Physical devices and systems within the organization are inventoried	No Mapping
ID.AM-2: Software platforms and applications within the organization are inventoried	5.10.1.5 Cloud Computing
ID.AM-3: Organizational communication and data flows are mapped	5.1.3 Secondary Dissemination 5.1.4 Secondary Dissemination of Non-CHRI CJI 5.7.1.2 Network Diagram 5.10.1 Information Flow Enforcement
ID.AM-4: External information systems are catalogued	5.5.6.1 Personally Owned Information Systems 5.10.1.5 Cloud Computing
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	No Mapping
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum
ID.BE-1: The organization's role in the supply chain is identified and communicated	No Mapping
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	No Mapping
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	No Mapping
ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	No Mapping
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	No Mapping
ID.GV-1: Organizational cybersecurity policy is established and communicated	5.5 Access Control 5.9 Physical Protection MP-1
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	No Mapping
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	No Mapping
ID.GV-4: Governance and risk management processes address cybersecurity risks	No Mapping
ID.RA-1: Asset vulnerabilities are identified and documented	No Mapping
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	5.10.4.4 Security Alerts and Advisories
ID.RA-3: Threats, both internal and external, are identified and documented	No Mapping
ID.RA-4: Potential business impacts and likelihoods are identified	No Mapping
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	No Mapping
ID.RA-6: Risk responses are identified and prioritized	No Mapping
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	No Mapping
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	No Mapping
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	No Mapping
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	5.1.2.1 Managing Changes to Service Providers
ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	5.1.1.6 Agency User Agreements
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the	5.1.1 Information Exchange 5.1.1.1 Information Handling 5.1.1.2 State and Federal Agency User Agreements

Subcategory	CJIS 5.9
objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	5.1.1.3 Criminal Justice Agency User Agreements 5.1.1.4 Interagency and Management Control Agreements 5.10.1.5 Cloud Computing
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	5.1.2 Monitoring, Review, and Delivery of Services 5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division 5.11.1.2 Triennial Security Audits by the FBI CJIS Division 5.11.2 Audits by the CSA 5.11.3 Special Security Inquiries and Audits
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	No Mapping
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	5.5.1 Account Management 5.6 Identification and Authentication 5.6.3 Identifier and Authenticator Management 5.6.3.2 Authenticator Management 5.13.6 Access Control 5.13.7 Identification and Authentication 5.13.7.1 Local Device Authentication
PR.AC-2: Physical access to assets is managed and protected	5.9.1 Physically Secure Location 5.9.1.1 Security Perimeter 5.9.1.2 Physical Access Authorizations 5.9.1.3 Physical Access Control 5.9.1.4 Access Control for Transmission Medium 5.9.1.5 Access Control for Display Medium 5.9.1.6 Monitoring Physical Access 5.9.1.7 Visitor Control 5.9.1.8 Delivery and Removal 5.9.2 Controlled Area
PR.AC-3: Remote access is managed	5.5.6 Remote Access 5.5.6.2 Publicly Accessible Computers 5.10.1.5 Cloud Computing 5.13.1.2 Cellular Devices 5.13.1.2.1 Cellular Service Abroad 5.13.1.2.2 Voice Transmissions Over Cellular Devices
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	5.5.1 Account Management 5.5.2 Access Enforcement 5.5.2.1 Least Privilege 5.5.2.2 System Access Control 5.5.2.3 Access Control Criteria 5.5.2.4 Access Control Mechanisms 5.7.2 Security of Configuration Documentation 5.10.4.5 Information Input Restrictions
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	5.10.1.1 Boundary Protection 5.13.1.1 802.11 Wireless Protocols
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	5.5.3 Unsuccessful Login Attempts 5.5.4 System Use Notification 5.6.1 Identification Policy and Procedures 5.6.2 Authentication Policy and Procedures 5.6.2.1.1 Password 5.6.2.1.1.1 Basic Password Standards 5.6.2.1.1.2 Advanced Password Standards 5.6.2.1.2 Personal Identification Number (PIN) 5.6.3.1 Identifier Management 5.6.2.2 Advanced Authentication 5.13.7.3 Device Certificates
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	5.5.5 Session Lock 5.6.2.1 Standard Authenticators 5.6.2.1.1.2 Advanced Password Standards 5.6.2.1.3 One-time Passwords (OTP) 5.6.2.2.1 Advanced Authentication Policy and Rationale 5.6.4 Assertions 5.13.7.2 Advanced Authentication 5.13.7.2.1 Compensating Controls

Subcategory	CJIS 5.9
PR.AT-1: All users are informed and trained	5.2 Basic Security Awareness Training 5.2.1.1 Level One Security Awareness Training 5.2.1.2 Level Two Security Awareness Training 5.2.1.3 Level Three Security Awareness Training
PR.AT-2: Privileged users understand their roles and responsibilities	5.2.1.2 Level Two Security Awareness Training 5.2.1.3 Level Three Security Awareness Training 5.2.1.4 Level Four Security Awareness Training
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	5.2.1.4 Level Four Security Awareness Training
PR.AT-4: Senior executives understand their roles and responsibilities	No Mapping
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	5.2.1.1 Level One Security Awareness Training 5.2.1.2 Level Two Security Awareness Training 5.2.1.3 Level Three Security Awareness Training
PR.DS-1: Data-at-rest is protected	5.10.1.2.2 Encryption for CJI at Rest 5.10.1.5 Cloud Computing MP-2 MP-3 MP-4 MP-5 MP-6 MP-7
PR.DS-2: Data-in-transit is protected	5.10.1.2.1 Encryption for CJI in Transit
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	5.9.1.8 Delivery and Removal
PR.DS-4: Adequate capacity to ensure availability is maintained	5.10.3 Partitioning and Virtualization 5.10.3.1 Partitioning 5.10.3.2 Virtualization
PR.DS-5: Protections against data leaks are implemented	5.10.1.2 Encryption 5.10.1.2.3 Public Key Infrastructure (PKI) Technology 5.10.1.5 Cloud Computing
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	5.10.4.1 Patch Management
PR.DS-7: The development and testing environment(s) are separate from the production environment	No Mapping
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	No Mapping
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	5.7.1.1 Least Functionality 5.13.3 Wireless Device Risk Mitigations 5.13.4 System Integrity
PR.IP-2: A System Development Life Cycle to manage systems is implemented	5.10.4.2 Malicious Code Protection 5.13.4.2 Malicious Code Protection
PR.IP-3: Configuration change control processes are in place	5.7.1 Access Restrictions for Changes
PR.IP-4: Backups of information are conducted, maintained, and tested	No Mapping
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	No Mapping
PR.IP-6: Data is destroyed according to policy	MP-6
PR.IP-7: Protection processes are improved	No Mapping
PR.IP-8: Effectiveness of protection technologies is shared	No Mapping
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	5.3 Incident Response 5.13.5 Incident Response 5.13.6 Access Control
PR.IP-10: Response and recovery plans are tested	No Mapping
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	5.2.3 Security Training Records 5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI 5.12.2 Personnel Termination 5.12.3 Personnel Transfer 5.12.4 Personnel Sanctions

Subcategory	CJIS 5.9
PR.IP-12: A vulnerability management plan is developed and implemented	5.10.4.1 Patch Management 5.13.4.1 Patching/Updates
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	No Mapping
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	No Mapping
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	5.4 Auditing and Accountability 5.4.1 Auditable Events and Content (Information Systems) 5.4.1.1 Events 5.4.1.1.1 Content 5.4.2 Response to Audit Processing Failures 5.4.3 Audit Monitoring, Analysis, and Reporting 5.4.4 Time Stamps 5.4.5 Protection of Audit Information 5.4.6 Audit Record Retention 5.4.7 Logging NCIC and III Transactions 5.10.1.5 Cloud Computing
PR.PT-2: Removable media is protected and its use restricted according to policy	MP-1 MP-2 MP-3 MP-4 MP-5 MP-7
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	5.13.4.3 Personal Firewall
PR.PT-4: Communications and control networks are protected	5.10.1.3 Intrusion Detection Tools and Techniques 5.13.1.3 Bluetooth 5.13.1.4 Mobile Hotspots 5.13.2 Mobile Device Management (MDM)
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	No Mapping
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	No Mapping
DE.AE-2: Detected events are analyzed to understand attack targets and methods	No Mapping
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	No Mapping
DE.AE-4: Impact of events is determined	No Mapping
DE.CM-1: The network is monitored to detect potential cybersecurity events	No Mapping
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	No Mapping
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	No Mapping
DE.CM-4: Malicious code is detected	5.10.1.5 Cloud Computing 5.10.4.3 Spam and Spyware Protection
DE.CM-5: Unauthorized mobile code is detected	5.13 Mobile Devices
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	No Mapping
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	No Mapping
DE.CM-8: Vulnerability scans are performed	No Mapping
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	No Mapping
DE.DP-2: Detection activities comply with all applicable requirements	5.10.1.5 Cloud Computing
DE.DP-3: Detection processes are tested	No Mapping
DE.DP-4: Event detection information is communicated	No Mapping
DE.DP-5: Detection processes are continuously improved	No Mapping

Subcategory	CJIS 5.9
RS.RP-1: Response plan is executed during or after an incident	No Mapping
RS.CO-1: Personnel know their roles and order of operations when a response is needed	5.3.2 Management of Security Incidents 5.3.3 Incident Response Training
RS.CO-2: Incidents are reported consistent with established criteria	5.3.1 Reporting Security Events
RS.CO-3: Information is shared consistent with response plans	No Mapping
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	No Mapping
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	5.3.4 Incident Monitoring
RS.AN-1: Notifications from detection systems are investigated	No Mapping
RS.AN-2: The impact of the incident is understood	No Mapping
RS.AN-3: Forensics are performed	5.3.2.2 Collection of Evidence
RS.AN-4: Incidents are categorized consistent with response plans	No Mapping
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	No Mapping
RS.MI-1: Incidents are contained	No Mapping
RS.MI-2: Incidents are mitigated	No Mapping
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	No Mapping
RS.IM-1: Response plans incorporate lessons learned	No Mapping
RS.IM-2: Response strategies are updated	No Mapping
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	No Mapping
RC.IM-1: Recovery plans incorporate lessons learned	No Mapping
RC.IM-2: Recovery strategies are updated	No Mapping
RC.CO-1: Public relations are managed	No Mapping
RC.CO-2: Reputation is repaired after an incident	No Mapping
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	No Mapping