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. Agencies using cloud based services are required to make informed decisions on whether or not the cloud provider can offer services that maintain compliance with the requirements of the CJIS Security Policy.

This document outlines the specific security policies and practices for Axon Cloud Services and how they are compliant with the CJIS Security Policy, version 5.8. 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 (https://www.fbi.gov/services/cjis/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.

Axon has also provided 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/trust/compliance/cjis.

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

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
CJIS Security Policy Area 1 - Information Exchange Agreements					
5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums shall be protected with appropriate security safeguards.	Agency		
5.1.1	Information Exchange	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.	Agency	Agencies are responsible for establishing information exchange agreements with parties with whom they share data through Axon Cloud Services.	Axon's contractual agreement with the agency outlines the data protection roles, responsibilities, and data ownership.
	"	Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.	Agency		
	"	Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange.	Agency		
	"	Law Enforcement and civil agencies **shall** have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.	Agency		
5.1.1.1	Information Handling	Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse.	Agency	Agencies must establish policies related to the access and usage of data stored within Axon Cloud Services.	Axon maintains policies and practices within Axon Cloud Services for securely handling information.
	"	Using the requirements in this policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI.	Agency		
5.1.1.2	State and Federal Agency User Agreements	Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this policy before accessing and	Agency	CSA heads or SIB Chiefs are responsible for maintaining this written agreement.	N/A

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		participating in CJIS records information programs.			
	"	This agreement shall include the standards and sanctions governing utilization of CJIS systems.	Agency		
	"	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.	Agency		
	"	All user agreements with the FBI CJIS Division **shall** be coordinated with the CSA head.	Agency		
5.2	Policy Area 2: Basic Security Awareness Training	Basic security awareness training shall be required within six months of initial assignment and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location.	Both	Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.	Axon maintains a comprehensive security awareness program which includes annual training. Authorized Axon personnel with access to CJI are required to complete Level 4 CJIS Security Training upon assignment and biennially thereafter.
5.2.1.1	Level One Security Awareness Training	At a minimum, the following topics **shall** be addressed as baseline security awareness training for all personnel who have access to a physically secure location:		Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.	See 5.2
	"	1. Individual responsibilities and expected behavior with regard to being in the vacinity of CJI usage and/or terminals.	Both		
	"	2. Implications of noncompliance.	Both		
	"	3. Incident response (Identify points of contact and individual actions).	Both		
	"	4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.2.1.2	Level Two Security Awareness Training	In addition to 5.2.1.1 above, the following topics, at a minimum, **shall** be addressed as baseline security awareness training for all authorized personnel with access to CJI:		Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.	See 5.2
	"	1. Media Protection.	Both		
	"	2. Protect information subject to confidentiality concerns — hardcopy through destruction.	Both		
	"	3. Proper handling and marking of CJI.	Both		
	"	4. Threats, vulnerabilities, and risks associated with handling of CJI.	Both		
	"	5. Social engineering.	Both		
	"	6. Dissemination and destruction.	Both		
5.2.1.3	Level Three Security Awareness Training	In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:		Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.	See 5.2
	"	1. Rules that describe responsibilities and expected behavior with regard to information system usage.	Both		
	"	2. Password usage and management—including creation, frequency of changes, and protection.	Both		
	"	3. Protection from viruses, worms, Trojan horses, and other malicious code.	Both		
	"	4. Unknown e-mail/attachments.	Both		
	"	5. Web usage—allowed versus prohibited; monitoring of user activity.	Both		
	"	6. Spam.	Both		
	"	7. Physical Security—increases in risks to systems and data.	Both		
	"	8. Handheld device security issues—address both physical and wireless security issues.	Both		
	"	9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		technical contact for assistance.			
	"	10. Laptop security—address both physical and information security issues.	Both		
	"	11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).	Both		
	"	12. Access control issues—address least privilege and separation of duties.	Both		
	"	13. Individual accountability—explain what this means in the agency.	Both		
	"	14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.	Both		
	"	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.	Both		
	"	16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.	Both		
	"	17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.	Both		
5.2.1.4	Level Four Security Awareness Training	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.):		Agencies are responsible for ensuring personnel who access Axon Cloud Services undergo appropriate security awareness training.	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
	"	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.	Both		
	"	2. Data backup and storage—centralized or decentralized approach.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	3. Timely application of system patches—part of configuration management.	Both		biennially.
	"	4. Access control measures.	Both		
	"	5. Network infrastructure protection measures.	Both		
5.2.2	LASO Training	LASO training shall be required prior to assuming duties but no later than six months after initial assignment and annually thereafter.		Agencies are responsible for training LASO	N/A
	"	At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:	Both		
	"	1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.	Both		
	"	2. Additional state/local/tribal/federal agency LASO roles and responsibilities	Both		
	"	3. Summary of audit findings from previous state audits of local agencies.	Both		
	"	4. Findings from the last FBI CJIS Division audit of the CSA.	Both		
	"	5. Most recent changes to the CJIS Security Policy	Both		
5.2.3	Security Training Records	Records of individual basic security awareness training and specific information system security training **shall** be:		Agencies are responsible for maintaining records of security awareness training for personnel who access Axon Cloud Services.	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
		- documented			
		- kept current			
		- maintained by the CSO/SIB/Compact Officer			

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
					Online training at Level 4 biennially. Records of training can be provided to customers.
CJIS Security Policy Area 3 - Incident Response					
5.3	Policy Area 3: Incident Response	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…	Both	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.	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.
	"	...(ii) track, document, and report incidents to appropriate agency officials and/or authorities.	Both		
	"	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.	Both		
5.3.1	Reporting Security Events	The agency shall promptly report incident information to appropriate authorities.	Both	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 will notify customer administrators registered on Axon Cloud Services within 72 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.
	"	Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken.	Both		
	"	Formal event reporting and escalation procedures shall be in place.	Both		
	"	Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents.	Both		
	"	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	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		quickly as possible to the designated point of contact.			
5.3.1.1.1	FBI CJIS Division Responsibilities	The FBI CJIS Division **shall**:		Applicable to FBI CJIS Division only.	Applicable to FBI CJIS Division only.
	"	1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).	CJIS/CSO		
	"	2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.	CJIS/CSO		
	"	3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.	CJIS/CSO		
	"	4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.	CJIS/CSO		
	"	5. Track all reported incidents and/or trends.	CJIS/CSO		
	"	6. Monitor the resolution of all incidents.	CJIS/CSO		
5.3.1.1.2	CSA ISO Responsibilities	The CSA ISO **shall**:		Applicable to CSA ISO responsibilities only.	Applicable to CSA ISO responsibilities only.
	"	1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.	CJIS/CSO		
	"	2. Identify individuals who are responsible for reporting incidents within their area of responsibility.	CJIS/CSO		
5.3.1.1.2	"	3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.	CJIS/CSO		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.	CJIS/CSO		
	"	5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.	CJIS/CSO		
	"	6. Act as a single POC for their jurisdictional area for requesting incident response assistance.	CJIS/CSO		
5.3.2	Management of Security Incidents	A consistent and effective approach **shall** be applied to the management of security incidents.	Both	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 maintains security incident response procedures and capabilities for Axon Cloud Services. Details can be found within Axon's SOC 2+ report upon request.
	"	Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.	Both		
5.3.2.1	Incident Handling	The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	Both	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 maintains security incident response procedures and capabilities for Axon Cloud Services. Details can be found within Axon's SOC 2+ report upon request.
	"	Wherever feasible, the agency **shall** employ automated mechanisms to support the incident handling process.	Both		
5.3.2.2	Collection of Evidence	Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	Both	Agencies are responsible for establishing incident response capabilities and must report to Axon if they believe an unauthorized third party may be using their	Axon maintains security incident response procedures and capabilities for Axon Cloud Services, which include requirements to collect and

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
				account or their content, or if their account information is lost or stolen.	maintain appropriate evidence, when necessary.
5.3.3	Incident Response Training	The agency **shall** ensure general incident response roles responsibilities are included as part of required security awareness training.	Both	Agencies are responsible for establishing incident response capabilities and including general incident response roles and responsibilities in security awareness training.	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.
5.3.4	Incident Monitoring	The agency **shall** track and document security incidents on an ongoing basis.	Both	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 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.
	"	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).	Both	Applicable to CSA ISO responsibilities only.	Applicable to CSA ISO responsibilities only.
CJIS Security Policy Area 4 - Auditing and Accountability					
5.4	Policy Area 4: Auditing and Accountability	Agencies **shall** implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.	Service Provider	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.	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.
	"	Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.	Service Provider		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.4.1	Auditable Events and Content (Information Systems)	The agency's information system **shall** generate audit records for defined events.	Service Provider	N/A	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.
	"	The agency **shall** specify which information system components carry out auditing activities.	Service Provider		
	"	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.	Service Provider		
	"	The agency **shall** periodically review and update the list of agency-defined auditable events.	Service Provider		
	"	In the event an agency does not use an automated system, manual recording of activities **shall** still take place.	Service Provider		
5.4.1.1	Events	The following events **shall** be logged:		Within the Axon Cloud Services, detailed usage and access reports are available for agencies to monitor their accounts.	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.
	"	1. Successful and unsuccessful system log-on attempts.	Service Provider		
	"	2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.	Service Provider		
	"	3. Successful and unsuccessful attempts to change account passwords.	Service Provider		
	"	4. Successful and unsuccessful actions by privileged accounts.	Service Provider		
	"	5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.	Service Provider		
5.4.1.1.1	Content	The following content **shall** be included with every audited event:			In alignment with the Axon Information Security program, Axon Cloud Services systems are configured to log all required
	"	1. Date and time of the event.	Service Provider	N/A	

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	2.The component of the information system (e.g., software component, hardware component) where the event occurred.	Service Provider		events and more to a central logging system. This includes date and time of the event, user identity, outcome of the event, where the event occurred, and type of event.
	"	3. Type of event.	Service Provider		
	"	4. User/subject identity.	Service Provider		
	"	5. Outcome (success or failure) of the event.	Service Provider		
5.4.2	Response to Audit Processing Failures	The agency's information system **shall** provide alerts to appropriate agency officials in the event of an audit processing failure.	Both	Within the Axon Cloud Services application, detailed usage and access reports are available for agencies to monitor their accounts.	Controls are established to alert Axon of any log collection or processing failures.
5.4.3	Audit Monitoring, Analysis, and Reporting	The responsible management official **shall** designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.	Both	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 employs advanced detection and analysis capabilities of system events for Axon Cloud Services. This includes automated detection and alerts for unusual activity or attacks.
	"	Audit review/analysis **shall** be conducted at a minimum once a week.	Both		
	"	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.	Both		
5.4.4	Time Stamps	The agency's information system **shall** provide time stamps for use in audit record generation.	Service Provider	N/A	The Axon Cloud Services central logging system collects event generation time and event

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	The time stamps **shall** include the date and time values generated by the internal system clocks in the audit records.	Service Provider		received time. All systems are synchronized to an internal clock. Customer logs within Axon Cloud Services also include timestamps synchronized to an internal clock.
	"	The agency shall synchronize internal information system clocks on an annual basis.	Service Provider		
5.4.5	Protection of Audit Information	The agency's information system **shall** protect audit information and audit tools from modification, deletion and unauthorized access.	Service Provider	N/A	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.
5.4.6	Audit Record Retention	The agency **shall** retain audit records for at least one (1) year.	Service Provider	N/A	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.
	"	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.	Service Provider		
5.4.7	Logging NCIC and III Transactions	A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions.	Service Provider		Not applicable to Axon Cloud Services as Axon does not conduct NCIC and III transactions.
	"	The III portion of the log shall clearly identify both the operator and the authorized receiving agency.	Agency	N/A	

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	III logs shall also clearly identify the requester and the secondary recipient.	Agency		
	"	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.	Agency		
CJIS Security Policy Area 5 - Access Control					
5.5.1	Account Management	The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.	Both	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 maintains account management policies and practices for Axon Cloud Services systems including at least quarterly account validation.
	"	The agency shall validate information system accounts at least annually and…	Both		
	"	...and **shall** document the validation process.	Both		
	"	The agency shall identify authorized users of the information system and specify access rights/privileges.	Both		
	"	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.	Both		
	"	2. Satisfaction of all personnel security criteria.	Both		
	"	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.	Both		
	"	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.	Both		
5.5.2	Access Enforcement	The information system shall enforce assigned authorizations for controlling access to the system and contained information.	Both	Agencies are responsible for implementing this control for their user access into Axon Cloud Services. Within Axon Cloud Services roles and permissions are customizable	Axon has documented and implemented logical access controls to enforce session control, authorization, multi-factor and remote access requirements. Individuals are
	"	The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		relevant information to explicitly authorized personnel.		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.	assigned unique User IDs when accessing Axon systems. Axon account management practices and implementation is designed according to the principle of least privilege.
	"	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.	Both		
5.5.2.1	Least Privilege	The agency **shall** approve individual access privileges and…	Both	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 account management practices and implementation are designed according to the principle of least privilege.
	"	…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.	Both		
	"	The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.	Both		
	"	The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.	Both		
	"	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.	Both		
5.5.2.2	System Access Control	Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.	Both	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	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.
	"	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	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		accessing CJI, unless the agency grants authority based upon operational business needs.		as well as restricting concurrent active sessions.	Axon Cloud Services restrict the use of concurrent active sessions.
	"	(1. continued) Agencies **shall** document the parameters of the operational business needs for multiple concurrent active sessions.	Both		
	"	2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.	Both		
5.5.2.3	Access Control Criteria	Agencies shall control access to CJI based on one or more of the following:		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 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.
	"	1. Job assignment or function (i.e., the role) of the user seeking access.	Both		
	"	2. Physical location.	Both		
	"	3. Logical location.	Both		
	"	4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).	Both		
	"	5. Time-of-day and day-of-week/month restrictions.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.5.2.4	Access Control Mechanisms	When setting up access controls, agencies shall use one or more of the following mechanisms:		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 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.
	"	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.	Both		
	"	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.	Both		
	"	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. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.1.2 for encryption requirements).	Both		
	"	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.	Both		
5.5.3	Unsuccessful Login Attempts	Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI).	Both	Agencies are required to enforce technical and administrative controls to restrict access to Axon Cloud Services. Axon Cloud	Axon Cloud Services access control mechanisms are maintained in compliance with the specific CJIS security requirements and enforce user

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	The system **shall** automatically lock the account/node for a 10 minute time period unless released by an administrator.	Both	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.	lockouts or deny attempts from malicious-appearing IPs.
5.5.4	System Use Notification	The information system **shall** display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.	Both	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 Cloud Services systems implements an approved system use notification in compliance with the specific CJIS security requirement.
	"	The system use notification message **shall**, at a minimum, provide the following information:			
	"	1. The user is accessing a restricted information system.	Both		
	"	2. System usage may be monitored, recorded, and subject to audit.	Both		
	"	3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.	Both		
	"	4. Use of the system indicates consent to monitoring and recording.	Both		
	"	The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and…	Both		
	"	...and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.	Both		
	"	Privacy and security policies shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.5.5	Session Lock	The information system **shall** prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and…	Both	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 Cloud Services system administration access control mechanisms are maintained in compliance with the specific CJIS security requirements.
	"	...and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Both		
	"	Users **shall** directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.	Both		
5.5.6	Remote Access	The agency shall authorize, monitor, and control all methods of remote access to the information system.	Both	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 maintains policies and practices for Axon Cloud Services that limit remote access to only required individuals and require at least two factors for authentication.
	"	The agency **shall** employ automated mechanisms to facilitate the monitoring and control of remote access methods.	Both		
	"	The agency shall control all remote accesses through managed access control points.	Both		
	"	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 system.	Both		
	"	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.	Both		
	"	2. The escort **shall** be familiar with the system/area in which the work is being performed.	Both		
	"	3. The escort shall have the ability to end the session at any time.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.	Both		
	"	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	Both		
5.5.6.1	Personally Owned Information Systems	A personally owned information system **shall not** be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.	Both	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 prohibits the usage of personally owned information systems to access, process, store, or transmit CJI.
	"	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.	Both		
5.5.6.2	Publicly Accessible Computers	Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention	Both	Axon Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence	Axon Cloud Services back-end system administration is prohibited from publicly accessible computers.

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		center computers, public library computers, public kiosk computers, etc.		including restricting access to a defined IP ranges which limits access to approved locations.	
CJIS Security Policy Area 6 - Identification and Authentication					
5.6	Policy Area 6: Identification and Authentication	The agency **shall** identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.	Both	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 maintains policies and practices for Axon Cloud Services for identifying and authenticating users before allowing access.
5.6.1	Identification Policy and Procedures	Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified.	Both	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 maintains policies and practices for Axon Cloud Services for identifying and authenticating users before allowing access. Additionally, all users are required to have unique login credentials.
	"	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.	Both		
	"	Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system.	Both		
	"	Agencies shall ensure that all user IDs belong to currently authorized users.	Both		
	"	Identification data **shall** be kept current by adding new users and disabling and/or deleting former users.	Both		
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction.	Agency	N/A	N/A
	"	The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.			
	"	Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.	Agency		
	"	Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.	Agency		
5.6.2	Authentication Policy and Procedures	Each individual's identity **shall** be authenticated at either the local agency, CSA, SIB or Channeler level.	Agency	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.	N/A
	"	The authentication strategy **shall** be part of the agency's audit for policy compliance.	Agency		
	"	The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services.	CJIS/CSO		N/A
	"	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.	CJIS/CSO		
5.6.2.1	Standard Authenticators	Users **shall not** be allowed to use the same password or PIN in the same logon sequence.	Both	Axon Cloud Services do not use a PIN for authentication.	Axon Cloud Services do not use a PIN for authentication.
5.6.2.1.1	Password	When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in	Both	Agencies must address this requirement by selecting which standard to use.	Axon Cloud Services use the basic password standards.

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		5.6.2.1.1.1, OR follow the advanced passwords standards in 5.6.2.1.1.2.			
5.6.2.1.1.1	Basic Password Standards	When agencies elect to follow the basic password standards, passwords **shall:**	Both	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 Cloud Services password complexity requirements are maintained in compliance with the basic password standards.
	"	1. Be a minimum length of eight (8) characters on all systems.	Both		
	"	2. Not be a dictionary word or proper name.	Both		
	"	3. Not be the same as the Userid.	Both		
	"	4. Expire within a maximum of 90 calendar days.	Both		
	"	5. Not be identical to the previous ten (10) passwords.	Both		
	"	6. Not be transmitted in the clear outside the secure location.	Both		
	"	7. Not be displayed when entered.	Both		
5.6.2.1.1.2	Advanced Password Standards	When agencies elect to follow the advanced password standards, follow the guidance below:	Both	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 Cloud Services password complexity requirements are maintained in compliance with the basic password standards.
	"	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).	Both		
	"	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.	Both		
	"	3. Verifiers shall maintain a list of “banned passwords” that contains values known to be commonly-used, expected, or compromised.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list.	Both		
	"	5. If the chosen password is found to be part of a "banned passwords" list, the Verifier shall:	Both		
	"	a. Advise the subscriber that they need to select a different password,	Both		
	"	b. Provide the reason for rejection, and	Both		
	"	c. Require the subscriber to choose a different password.	Both		
	"	6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.	Both		
	"	7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.	Both		
	"	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.	Both		
	"	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.	Both		
	"	a. The salt shall be at least 32 bits in length.	Both		
	"	b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.	Both		
	"	10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.	Both		
5.6.2.1.2	Personal Identification Number (PIN)	When agencies implement the use of a PIN as a standard authenticator, the PIN attributes **shall**	Both	Axon Cloud Services do not use a PIN for authentication.	Axon Cloud Services do not use a PIN for authentication.

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		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.			
		1. Be a minimum length of six (6) digits.	Both		
		2. Have no repeating digits (i.e., 112233).	Both		
		3. Have no sequential patterns (i.e., 123456).	Both		
		4. Not be the same as the Userid.	Both		
		5. Expire within a maximum of 365 days.	Both		
		6. Not be identical to the previous three (3) PINs.	Both		
		7. Not be transmitted in the clear outside the secure location.	Both		
		8. Not be displayed when entered.	Both		
5.6.2.1.3	One-time Passwords (OTP)	When agencies implement the use of an OTP as authenticator, the OTP shall meet the requirements described below.		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 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.
	"	a. Be a minimum of six (6) randomly generated characters.	Both		
	"	b. Be valid for a single session.	Both		
	"	c. If not used, expire within a maximum of five (5) minutes after issuance.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.6.2.2	Advanced Authentication	When user-based certificates are used for authentication purposes, they shall:		Axon Cloud Services do not use user-based certifications for authentication.	Axon Cloud Services requires at least two-factor authentication for all system administration access. Axon Cloud Services do not utilize user-based certifications for authentication.
	"	1. Be specific to an individual user and not to a particular device.	Both		
	"	2. Prohibit multiple users from utilizing the same certificate.	Both		
	"	3. Require the user to "activate" that certificate for each user in some manner (e.g., passphrase or user-specific PIN)	Both		
5.6.2.2.1	Advanced Authentication Policy and Rationale	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...	Both	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)	System administration access to Axon Cloud Services requires at least two-factor authentication.
	"	... or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access).	Both		
	"	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.	Both		
	"	The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).	Both		
	"	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.	Both		
5.6.3	Identifier and Authenticator Management	The agency **shall** establish identifier and authenticator management processes.	Both	Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.	Axon maintains policies and practices for Axon Cloud Services for Identifier and Authenticator management.

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.6.3.1	Identifier Management	In order to manage user identifiers, agencies **shall**:		Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.	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.
	"	1. Uniquely identify each user.	Both		
	"	2. Verify the identity of each user.	Both		
	"	3. Receive authorization to issue a user identifier from an appropriate agency official.	Both		
	"	4. Issue the user identifier to the intended party.	Both		
	"	5. Disable the user identifier after a specified period of inactivity.	Both		
	"	6. Archive user identifiers.	Both		
5.6.3.2	Authenticator Management	In order to manage information system authenticators, agencies shall:		Agencies must address this requirement through appropriate policies, procedures, and configurations in how they use Axon Cloud Services.	Axon maintains policies and practices for Axon Cloud Services for Identifier and Authenticator management through the Information Security Program.
	"	1. Define initial authenticator content.	Both		
	"	2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.	Both		
	"	3. Change default authenticators upon information system installation.	Both		
	"	4. Change/refresh authenticators periodically.	Both		
	"	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.	Both		
5.6.4	Assertions	Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:		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 Cloud Services do not remotely authenticate Axon personnel to Axon Cloud Services. As such, assertion mechanisms are not used.
	"	1. Digitally signed by a trusted entity (e.g., the identity provider).	Both		
	"	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	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		[TLS]) that cryptographically authenticates the verifier and protects the assertion.			
	"	Assertions generated by a verifier **shall** expire after 12 hours and…	Both		
	"	...and **shall not** be accepted thereafter by the relying party.	Both		
CJIS Security Policy Area 7 - Configuration Management					
5.7.1.1	Least Functionality	The agency shall configure the application, service, or information system to provide only essential capabilities and…	Both	Agencies are responsible for restricting and controlling changes made by agency personnel to their Axon Cloud Services.	Axon designs and maintains the Axon Cloud Services infrastructure under the principle of least functionality.
	"	...and **shall** specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.	Both		
5.7.1.2	Network Diagram	The agency **shall** ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.	Both	Agencies are responsible for maintaining their own system diagram that contains the Axon Cloud Services connection.	Axon maintains a current system diagram for Axon Cloud Services.
	"	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.	Both		
	"	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.	Both		
	"	3. “For Official Use Only” (FOUO) markings.	Both		
	"	4. The agency name and date (day, month, and year) drawing was created or updated.	Both		
5.7.2	Security of Configuration Documentation	Agencies **shall** protect the system documentation from unauthorized access	Both	Agencies are responsible for restricting and controlling	Axon system configuration documentation is classified as confidential and protected

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		consistent with the provisions described in section 5.5 Access Control.		access to system configuration documentation.	accordingly according to Axon's internal classification and detailed within Axon's Information Security Policy.
CJIS Security Policy Area 8 - Media Protection					
5.8	Policy Area 8: Media Protection	Media protection policy and procedures **shall** be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals.	Agency	Agencies are responsible for documenting and implementing policies regarding secure handling of data.	N/A
	"	Procedures shall be defined for securely handling, transporting and storing media.	Agency		
5.8.1	Media Storage and Access	The agency shall securely store electronic and physical media within physically secure locations or controlled areas.	Both	Agencies are responsible for documenting and implementing policies regarding secure handling of data.	Axon ensures digital evidence in Axon Cloud Services is stored in physically secure and controlled locations.
	"	The agency shall restrict access to electronic and physical media to authorized individuals.	Both		
	"	If physical and personnel restrictions are not feasible then the data shall be encrypted per section 5.10.1.2.	Both		
5.8.2	Media Transport	The agency **shall** protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.	Agency	Agencies are responsible for documenting and implementing policies regarding secure handling of data.	N/A
5.8.2.1	Electronic Media in Transit	Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.	Agency	Agencies are responsible for documenting and implementing policies regarding secure handling of data.	N/A
	"	Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency **shall** institute physical controls to ensure the security of the data.	Both		Axon maintains policies and practices for Axon Cloud Services for securely handling data. Sensitive communications and data that traverse public networks are encrypted. Data is encrypted in transit over public

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
					networks using a robust TLS 1.2 implementation with 256 Bit Perfect Forward Secrecy.
5.8.2.2	Physical Media in Transit	Physical media **shall** be protected at the same level as the information would be protected in electronic form.	Agency	Agencies are responsible for protecting any information from Axon Cloud Services put into physical form in the same manner as in electronic form.	N/A
5.8.3	Electronic Media Sanitization and Disposal	The agency **shall** sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.	Both	Agencies are responsible for documenting and implementing policies regarding electronic media sanitization and disposal of data outside of Axon Cloud Services.	Axon maintains practices for sanitizing and disposing of 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.
	"	Inoperable electronic media shall be destroyed (cut up, shredded, etc.).	Agency		N/A
	"	The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media.	Agency		
	"	Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.8.4	Disposal of Physical Media	Physical media shall be securely disposed of when no longer required, using formal procedures.	Agency	Agencies are responsible for documenting and implementing policies regarding secure handling of data.	N/A
	"	Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals.	Agency		
	"	Physical media **shall** be destroyed by shredding or incineration.	Agency		
	"	Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.	Agency		
CJIS Security Policy Area 9 - Physical Protection					
5.9	Policy Area 9: Physical Protection	Physical protection policy and procedures **shall** be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.	Both	Agencies are responsible for documenting and implementing policies regarding physical protection.	Axon maintains policies and practices for Axon Cloud Services related to physical protection.
5.9.1.1	Security Perimeter	The perimeter of physically secure location shall be prominently posted and separated from non-secure locations by physical controls.	Both	Agencies are responsible for maintaining a secure physical perimeter.	Axon defines and controls the physically secure perimeter for Axon facilities.
	"	Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.	Both		
5.9.1.2	Physical Access Authorizations	The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or…	Both	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 ensures physical access to secure locations is limited to authorized personnel.
	"	...or **shall** issue credentials to authorized personnel.	Both		
5.9.1.3	Physical Access Control	The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and…	Both	Agencies are responsible for restricting and controlling physical access to physical access points.	Axon regularly reviews the specific security practices and audit results documented by underlying infrastructure

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	...and **shall** verify individual access authorizations before granting access.	Both		providers to ensure the highest standards are met. Axon ensures physical access is limited to authorized personnel.
5.9.1.4	Access Control for Transmission Medium	The agency shall control physical access to information system distribution and transmission lines within the physically secure location.	Both	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 restricts and monitors access to transmission lines within the physically secure locations used to deliver Axon Cloud Services.
5.9.1.5	Access Control for Display Medium	The agency **shall** control physical access to information system devices that display CJI and…	Both	Agencies should maintain policy and procedure surrounding the devices used to access Axon Cloud Services.	Axon maintains policy and procedure surrounding the devices used to administer Axon Cloud Services.
	"	...and **shall** position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.	Both		
5.9.1.6	Monitoring Physical Access	The agency shall monitor physical access to the information system to detect and respond to physical security incidents.	Both	Agencies are responsible for restricting and controlling physical access to locations managed by agencies to support the use of Axon Cloud Services.	Axon maintains policies and practices for monitoring physical access and responding to suspicious events.
5.9.1.7	Visitor Control	The agency **shall** control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).	Both	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 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.
	"	The agency **shall** escort visitors at all times and monitor visitor activity.	Both		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.9.1.8	Delivery and Removal	The agency **shall** authorize and control information system-related items entering and exiting the physically secure location.	Both	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.	Axon maintains policies and practices for controlling information-system-related items.
5.9.2	Controlled Area	If an agency cannot meet all of the controls required for establishing a physically secure location but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a "controlled area" for the purpose of day-to-day CJI access or storage.	Both	Agencies are responsible for documenting and implementing policies and practices related to physical protection.	Axon maintains policies and practices for Axon Cloud Services related to physical protection.
	"	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.	Both		
	"	2. Lock the area, room, or storage container when unattended.	Both		
	"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.	Both		
	"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJI.	Both		
CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity					
5.10.1	Information Flow Enforcement	The network infrastructure **shall** control the flow of information between interconnected systems.	Service Provider		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,

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
					including firewalls, ACLs, proxies, and load balancers.
5.10.1.1	Boundary Protection	The agency **shall**:			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.
	"	1. Control access to networks processing CJI.	Service Provider		
	"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.	Service Provider		
	"	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 5.10.4.4 for guidance on personal firewalls.	Service Provider		
	"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	Service Provider		
	"	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 **shall** "fail closed" vs. "fail open").	Service Provider		
	"	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.	Service Provider		
5.10.1.2.1	Encryption for CJ I in Transit	a) See Sections 5.13.1.2.2 and 5.10.2.	Service Provider		Data transmitted in Axon Cloud Services is encrypted with 128 bits or stronger. Axon's Cryptographic Module that provides for protection of data in
	"	b) Encryption shall not be required if the transmission medium meets all of the following requirements:			

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	i. The agency owns, operates, manages, or protects the medium.	Agency	Agencies are responsible for maintaining encryption for data in transit for data being sent to destinations other than Axon Cloud Services.	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.
	"	ii. Medium terminates within physically secure locations at both ends with no interconnections between.	Agency		
	"	iii. Physical access to the medium is controlled by the agency using the requirements in Section 5.9.1 and 5.12.	Agency		
	"	iv. 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.	Agency		
	"	v. With approval of the CSO.	Agency		
5.10.1.2.2	Encryption for CJI at Rest	a) When agencies implement encryption on CJI at rest, the passphrase to unlock the cipher **shall** meet the following requirements:			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
	"	i. Be at least 10 characters	Service Provider		
	"	ii. Not be a dictionary word	Service Provider		
	"	iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character	Service Provider		
	"	iv. Be changed when previously authorized personnel no longer require access	Service		
	"	b) Multiple files maintained in the same unencrypted folder **shall** have separate and distinct passphrases.	Service Provider		
	"	b) All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) **shall** be applied.	Service Provider		
5.10.1.2.3	Public Key Infrastructure (PKI) Technology	Registration to receive a public key certificate **shall**:			Axon uses PKI to provide server authentication to clients interacting with Axon Cloud

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	a) Include authorization by a supervisor or a responsible official.	Service Provider		Services. Axon's TLS certifications are signed by Rapid SSL. Rapid SSL verifies identity when issuing the certificate.
	"	b) Be accomplished by a secure process that verifies the identity of the certificate holder.	Service Provider		
	"	c) Ensure the certificate is issued to the intended party.	Service Provider		
5.10.1.3	Intrusion Detection Tools and Techniques	Agencies **shall**:	Service Provider		Axon Cloud Services employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks.
	"	1. Implement network-based and/or host-based intrusion detection or prevention tools.	Service Provider		
	"	2. Maintain current intrusion detection or prevention signatures.	Service Provider		
	"	3. Monitor inbound and outbound communications for unusual or unauthorized activities.	Service Provider		
	"	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.	Service Provider		
	"	5. Review intrusion detection or prevention logs weekly or implement automated event notification	Service Provider		
	"	6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	Service Provider		
5.10.1.4	Voice over Internet Protocol	In addition to the security controls described in this document, the following additional controls **shall** be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:			Not applicable to Axon Cloud Services security practices. VOIP is not used within Axon Cloud Services.

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	1. Establish usage restrictions and implementation guidance for VoIP technologies.	Service Provider		
	"	2. Document, monitor and control the use of VoIP within the agency.	Service Provider		
	"	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.	Service Provider		
5.10.1.5	Cloud Computing	The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).	Service Provider		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.
	"	Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and…	Service Provider		
	"	...and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	Service Provider		
5.10.2	Facsimile Transmission of CJI	CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.	Service Provider		Not applicable to Axon Cloud Services security practices. Facsimile transmission is not utilized in Axon Cloud Services.
5.10.3.1	Partitioning	The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.	Service Provider		Axon Cloud Services uses many partitioning and segmentation methods for security purposes. These include network segmentation, OS separation,
	"	The application, service, or information system shall physically or logically separate user	Service Provider		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		interface services (e.g. public Web pages) from information storage and management services (e.g. database management).			firewalls, and logical access separation.
5.10.3.2	Virtualization	In addition to the security controls described in this policy, the following additional controls shall be implemented in a virtual environment:			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.
	"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.	Service Provider		
	"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.	Service Provider		
	"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally or be separated by a virtual firewall.	Service Provider		
	"	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.	Service Provider		
	"	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.	Service Provider		
	"	2. Encrypt network traffic within the virtual environment.	Service Provider		
5.10.4.1	Patch Management	The agency shall identify applications, services, and information systems containing software or components affected by recently announced	Service Provider		Axon Cloud Services ensures policies and procedures are established to ensure patches are

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		software flaws and potential vulnerabilities resulting from those flaws.			applied within defined timeframes. Servers are patched according to the Evidence.com Patch Policy.
	"	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.	Service Provider		
	"	Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.	Service Provider		
5.10.4.2	Malicious Code Protection	The agency **shall** implement malicious code protection that includes automatic updates for all systems with Internet access.	Service Provider		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.
	"	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).	Service Provider		
	"	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.	Service Provider		
	"	The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.	Service Provider		
5.10.4.3	Spam and Spyware Protection	The agency **shall** implement spam and spyware protection.	Service Provider		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
	"	The agency **shall**:			
	"	1. Employ spam protection mechanisms at critical information system entry points (e.g.	Service Provider		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		firewalls, electronic mail servers, remote-access servers).			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.
	"	2. Employ spyware protection at workstations, servers and mobile computing devices on the network.	Service Provider		
	"	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 document.	Service Provider		
5.10.4.4	Security Alerts and Advisories	The agency **shall**:			
	"	1. Receive information system security alerts/advisories on a regular basis.	Service Provider		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.
	"	2. Issue alerts/advisories to appropriate personnel.	Service Provider		
	"	3. Document the types of actions to be taken in response to security alerts/advisories.	Service Provider		
	"	4. Take appropriate actions in response.	Service Provider		
	"	5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	Service Provider		
5.10.4.5	Information Input Restrictions	The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.	Agency	The Agency is responsible for restricting the information input to any connection to FBI CJIS services to authorized personnel only.	N/A
CJIS Security Policy Area 11 - Formal Audits					

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.	CJIS/CSO	Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
	"	This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.	CJIS/CSO		
	"	The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	CJIS/CSO		
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	This audit **shall** include a sample of CJAs and NCJAs.	CJIS/CSO	Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
5.11.2	Audits by the CSA	Each CSA **shall**:		Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
	"	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.	CJIS/CSO		
	"	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.	CJIS/CSO		
	"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	CJIS/CSO		
	"	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.	CJIS/CSO		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.11.3	Special Security Inquiries and Audits	All agencies having access to CJI **shall** permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.	CJIS/CSO	Agencies are required to schedule and execute audits of Axon Cloud Services in compliance with the CJIS Security Policy.	Axon is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
	"	The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division.	CJIS/CSO		
	"	All results of the inquiry and audit **shall** be reported to the APB with appropriate recommendations.	CJIS/CSO		
CJIS Security Policy Area 12 - Personnel Security					
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing).	Agency	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.	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.
	"	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.	Agency		
	"	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.	Agency		
	"	2. All requests for access **shall** be made as specified by the CSO.	Agency		
	"	All CSO designees shall be from an authorized criminal justice agency.	Agency		
	"	3. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		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.	Agency		
	"	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	Agency		
	"	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.	Agency		
	"	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.	Agency		
	"	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...	Agency		
	"	...and the person's appointing authority shall be notified in writing of the access denial.	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and...	Agency		
	"	...and shall, upon request, provide a current copy of the access list to the CSO.	Agency		
5.12.2	Personnel Termination	Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI.	Both	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.	Axon maintains policies and practices for access management related to termination or transfer of employees.
	"	Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated.	Both		
	"	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.	Both		
5.12.3	Personnel Transfer	The agency **shall** review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.	Both	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.	Axon maintains policies and practices for access management related to termination or transfer of employees.
5.12.4	Personnel Sanctions	The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.	Both	Agencies must address this control for users to whom they grant access to their instance of Axon Cloud Services.	Axon maintains a formal sanction process for employees failing to comply with established security policies and practices.
CJIS Security Policy Area 13 - Mobile Devices					
5.13	Mobile Devices	The agency **shall**:		Agencies must address this requirement through appropriate policies and procedures. Axon Cloud Services provides many security features and capabilities to enable customers to securely	N/A
	"	(i) establish usage restrictions and implementation guidance for mobile devices;	Agency		
	"	(ii) authorize, monitor, control wireless access to the information system.	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
				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).	
5.13.1.1	802.11 Wireless Protocols	Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-80.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
	"	Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:	Agency		
	"	Agencies **shall** implement the following controls for all agency-managed wireless access points:			
	"	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.	Agency		
	"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	Agency		
	"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Agency		
	"	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.	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.	Agency		
	"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.	Agency		
	"	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.	Agency		
	"	8. Change the default service set identifier (SSID) in the APs.	Agency		
	"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Agency		
	"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.	Agency		
	"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.	Agency		
	"	10. Ensure that encryption key sizes are at least 128-bits and…	Agency		
	"	...and the default shared keys are replaced by unique keys.	Agency		
	"	11. Ensure that the ad hoc mode has been disabled.	Agency		
	"	12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the management interface.	Agency		
	"	13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS,	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
		etc.). Disable non-FIPS compliant secure access to the management interface.			
	"	14. Enable logging (if supported) and…	Agency		
	"	...and review the logs on a recurring basis per local policy.	Agency		
	"	At a minimum logs **shall** be reviewed monthly.	Agency		
	"	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.	Agency		
	"	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.	Agency		
5.13.1.2.1	Cellular Service Abroad	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.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
5.13.1.3	Bluetooth	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.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
5.13.1.4	Mobile Hotspots	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:		Agencies must address this requirement through appropriate policies and procedures.	N/A
	"	1. Enable encryption on the hotspot	Agency		
	"	2. Change the hotspot's default SSID	Agency		
	"	a. Ensure the hotspot SSID does not identify the device make/model or agency ownership	Agency		
	"	3. Create a wireless network password (Pre-shared key)	Agency		
	"	4. Enable the hotspot's port filtering/blocking features if present	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	5. Only allow connections from agency controlled devices	Agency		
	"	OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above.	Agency		
5.13.2	Mobile Device Management (MDM)	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 at any time.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
	"	Agencies **shall** implement the following controls when allowing CJI access from devices running limited feature operating system:			
	"	1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	Agency		
	"	2. MDM with centralized administration configured and implemented to perform at least the following controls:	Agency		
	"	i. Remote locking of the device	Agency		
	"	ii. Remote wiping of the device	Agency		
	"	iii. Setting and locking device configuration	Agency		
	"	iv. Detection of "rooted" and "jailbroken" devices	Agency		
	"	v. Enforcement of folder or disk level encryption	Agency		
	"	vi. Application of mandatory policy settings on the device	Agency		
	"	vii. Detection of unauthorized configurations	Agency		
	"	viii. Detection of unauthorized software or applications	Agency		
	"	ix. Ability to determine location of agency controlled devices	Agency		
	"	x. Prevention of unpatched devices from accessing CJI or CJI systems	Agency		
	"	xi. Automatic device wiping after a specified number of failed access attempts	Agency		
5.13.3	Wireless Device Risk Mitigations	Organizations **shall**, as a minimum, ensure that wireless devices:		Agencies must address this requirement through	N/A

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
				appropriate policies and procedures.	
	"	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.	Agency		
	Wireless Device Risk Mitigations (continued)	2. Are configured for local device authentication (see Section 5.13.8.1).	Agency		
	"	3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.	Agency		
	"	4. Encrypt all CJI resident on the device.	Agency		
	"	5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.	Agency		
	"	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.	Agency		
	"	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.	Agency		
5.13.4.1	Patching/Updates	Agencies shall monitor mobile devices to ensure their patch and update state is current.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
5.13.4.2	Malicious Code Protection	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.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
5.13.4.3	Personal Firewall	A personal firewall shall be employed on all devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems).	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
	"	At a minimum, the personal firewall shall perform the following activities:			
	"	1. Manage program access to the Internet.	Agency		
	"	2. Block unsolicited requests to connect to the PC.	Agency		
	"	3. Filter Incoming traffic by IP address or protocol.	Agency		
	"	4. Filter Incoming traffic by destination ports.	Agency		
	"	5. Maintain an IP traffic log.	Agency		
5.13.5	Incident Response	In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
	"	Special reporting procedures for mobile devices shall apply in any of the following situations:			
	"	1. Loss of device control. For example:	Agency		
	"	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	Agency		
	"	3. Device compromise	Agency		
	"	4. Device loss or compromise outside the United States	Agency		
5.13.6	Access Control	Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.13.7.1	Local Device Authentication	When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
	"	The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.	Agency		
5.13.7.2	Advance Authentication	When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
5.13.7.2.1	Compensating Controls	Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2.	Agency	Agencies must address this requirement through appropriate policies and procedures.	N/A
	"	The compensating controls shall:			
	"	1. Meet the intent of the CJIS Security Policy AA requirement	Agency		
	"	2. Provide a similar level of protection or security as the original AA requirement	Agency		
	"	3. Not rely upon the existing requirements for AA as compensating controls	Agency		
	“	4. Expire upon the CSO approved date or when a compliant AA solution is implemented.	Agency		
	"	The following minimum controls shall be implanted as a part of the CSO approved compensating controls	Agency		
	"	Possession and registration of the agency-issued smartphone or tablet as an indication it is the authorized user	Agency		
	"	Use of device certificates as per Section 5.13.7.3 Device Certificates	Agency		
	"	Implemented CJIS Security Policy compliant standard authenticator protection on the secure device	Agency		

Control number	Topic	Shall Statement	Responsibility (SaaS Model)	Agency Details	Axon Details
5.13.7.3	Device Certificates	When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:		Agencies must address this requirement through appropriate policies and procedures.	N/A
	"	1. Protected against being extracted from the device	Agency		
	"	2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts	Agency		
	"	3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use	Agency		

CJIS Security Policy Appendix G.3 Cloud Computing

As stated in the CJIS Security Policy, the following questions can help frame the process of determining compliance (of a cloud provider) with the existing requirements of the CJIS Security Policy. The following outlines Axon's response to the questions.

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?	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? (5.8 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.