AWS
Criminal Justice Information Services (CJIS)

Workbook

November 2015

(CJIS Security Policy Version 5.4)

amazon web services

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Workbook Introduction

The Amazon Web Services (AWS) cloud environment is designed with security in mind and may be utilized by customers to satisfy a wide range of regulatory requirements, including the Criminal Justice Information Services (CJIS) Security Policy. This document provides an overview of the CJIS Security Policy, details specific requirements, and answers commonly asked questions about AWS and CJIS Security Policy to support customers seeking to build solutions compliant with CJIS Security Policy on AWS.

Moreover, this document also serves as a template for customers to document their implementation of the CJIS requirements alongside AWS' response and should be used to submit to their authorizing agency. A formal CJIS "certification" or authorization is granted by the agency (e.g. State, County or City) being supported and as such that authorization is subject to the individual agency's application of the CJIS security requirements. AWS' secure infrastructure may allow customers with CJIS security requirements to build an environment compliant with CJIS Security Policy requirements using AWS services.

Per the CJIS security policy AWS is committed to the premise of full lifecycle security of CJI; which is the basis of our CJIS Security Policy workbook:

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

Abstract

This workbook outlines the shared responsibility between AWS and the CJIS partner and/or direct customer agency on how AWS directly supports the CJIS Security Policy (**Version 5.4 10/06/2015**) and the requirements within our FedRAMP accreditation, which is based on NIST 800-53rev4.

Per the CJIS Advisory Policy Board (APB) Security & Access (SA) Subcommittee, the CJIS to NIST 800-53rev4 requirements (**Version 5.4 10/06/2015**), have been mapped to the requirements of the CJIS Security Policy. NIST 800-53rv4 are base controls for Federal Risk and Authorization Management Program (FedRAMP).

This document and our approach has been reviewed by the CJIS APB subcommittee chairmen, partners in the CJIS space, and FBI CJIS IT Auditors with favorable support on the efficacy of our workbook and approach.

What is FedRAMP?

The U.S. Federal Risk and Authorization Management Program (FedRAMP^{sm}) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" model to ensure cloud based services have adequate information security, eliminate duplication of effort, reduce risk management costs, and accelerate government-wide cloud adoption. FedRAMP conforms to the National Institute of Science & Technology (NIST) 800 Series Special Publications to verify that all authorizations are compliant with Federal Information Security Management Act (FISMA).

CJIS Security Policy Cloud Guidance

CJIS Security Policy, Appendix G, Table 1 (p. 155) summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a cloud service arrangement.

#	Area	Recommendation
1	Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
2	Compliance	• Understand the various types of laws and regulations in addition to CJIS requirements that impose security and privacy obligations on the customer organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy, and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
3	Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support ongoing risk management decisions.
4	Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
5	Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

#	Area	Recommendation
6	Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
7	Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. • Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represents significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
8	Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
9	Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information both during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

Creating a CJIS Environment on AWS

Example: CJIS Use Case (Partner Solution)

AWS has several partner solutions, which collect, transfers, manage as well as share digital evidence (e.g., video and audio files) related to law enforcement interactions. AWS is also working with several partners who are delivering electronic warrant services as well as other unique CJIS law enforcement applications and services directly or indirectly to CJIS customers as illustrated above.

As referenced from the CJIS security policy AWS utilizes a **shared responsibility** between AWS, our partners and our customers.

> *"Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI)."*

Similar to our other compliance frameworks, using a cloud service, which aligns to CJIS security requirements, ***doesn't*** mean that your environment automatically adheres to applicable CJIS requirements. It's up to you (or your AWS partner/systems integrator) to architect a solution that meets applicable CJIS requirements.

One of the changes made within the updated CJIS Security Policy is the risk verse realism approach of applying risk-based approaches can be used to mitigate risks based on

> ***"2.3 Risk Versus Realism***
>
> *Every "shall" statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum-security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements."*

One advantage of using AWS for CJIS workloads is the CJI owners (agencies) inherit a significant portion of the security control implementation from AWS and the partner solution for addressing and meeting CJIS security policy elements.

AWS customers and partners should enable several security features, functions and utilize leading practices in-order to create a CJIS compliant environment within their use of AWS. The following section provides a high-level overview of services and tools for agencies and partners should consider as part of their CJIS implementation on AWS:

System and Communication Protection and Information Integrity

(Ref. CJIS Policy Area 10)

- AWS Virtual Private Cloud (VPC) - VPC allows customers to connect existing infrastructure to a set of logically isolated AWS compute resources via a Virtual Private Network (VPN) connection, and to extend existing management capabilities such as security services, firewalls, and intrusion detection systems to include virtual resources built on AWS.
- AWS Direct Connect (DX) - Implementing AWS DX makes it possible to establish dedicated network connections between the customer network and an AWS DX location.
- *Perfect Forward Secrecy* – For even greater communication privacy, several AWS services such as AWS Elastic Load Balancer and Amazon CloudFront offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use Perfect Forward Secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.
- **Protect data in transit -** Customers should implement SSL encryption on their server instances. Customers will need a certificate from an external certification authority like VeriSign or Entrust. The public key included in the certificate authenticates each session and serves as the basis for creating the shared session key used to encrypt the data.

Identification and Authentication

(Ref. CJIS Policy Area 6)

- **Access Control** - IAM is central to securely controlling access to AWS resources. Administrators can create users, groups, and roles with specific access policies to control the actions that users and applications can perform through the AWS Management Console or AWS API. Federation allows IAM roles to be mapped to permissions from central directory services.

- IAM configuration - Creating user groups and assignment of rights, including creation of groups for internal auditors, an IAM super user, and application administrative groups segregated by functionality (e.g., database and Unix administrators).

- AWS Multi-Factor Authentication (MFA) - A simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have).

- AWS Account Password Policy Settings – Within the IAM console under account settings a password policy can be set which supports the password policy requirements as outlined within the CJIS security policy.

Configuration Management

(Ref. CJIS Policy Area 7)

- **Amazon EC2** - is a web service that provides resizable compute capacity in the cloud. It provides you with complete control of your computing resources and lets you run Amazon Machine Images (AMI).

- Amazon Machine Image (AMI) - provides the information required to launch an instance, which is a virtual server in the cloud. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. You can also launch instances from as many different AMIs as you need.

- Amazon Machine Images (AMIs) management - Organizations commonly ensure security and compliance by centrally providing workload owners with pre-built AMIs. These "golden" AMIs can be preconfigured with host-based security software and hardened based on predetermined security guidelines. Workload owners and developers can then use the AMIs as starting images on which to install their own software and configuration, knowing the images are already compliant.

- Choosing an AMI **-** While AWS does provide images that can be used for deployment of host operating systems, AWS customers need to develop and implement system configuration and hardening standards to align with all applicable CJIS requirements for their operating systems.

- AWS EC2 Security Groups – You can control how accessible your virtual instances in EC2 are by configuring built-in firewall rules (Security Groups) – from totally public to completely private, or somewhere in between.

- Resource Tagging - Almost all AWS resources allow the addition of user-defined tags. These tags are metadata and irrelevant to the functionality of the resource, but are critical for cost management and access control. When multiple groups of users or multiple workload owners exist within the same AWS account, restricting access to resources based on tagging is important. Regardless of account structure, tag-based IAM policies can be used to place extra security restrictions on critical resources.

- AWS Config - Is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config service, you can immediately discover all of your AWS resources and view the configuration of each. You can receive notifications each time a configuration changes as well as dig into the configuration history to perform incident analysis.

- CloudFormation Templates - Creating preapproved AWS CloudFormation templates for common use cases. Using templates allows CJI workload owners to inherit the security implementation of the approved template, thereby limiting their authorization documentation to the features that are unique to their application. Templates can be reused to shorten the time required to approve and deploy new applications.

- AWS Service Catalog - Allows CJIS IT administrators to create, manage, and distribute portfolios of approved products to end users, who can then access the products they need in a personalized portal. Typical products include servers, databases, websites, or applications that are deployed using AWS resources (for example, an Amazon EC2 instance or an Amazon RDS database).

Media Protection & Information Integrity

(Ref. CJIS Policy Area 8 & 10)

- AWS Storage Gateway - The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organizations on-premises IT environment and AWS's storage infrastructure.

- *Storage* **-** AWS provides various options for storage of information including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3) and Amazon Relational Database Service (Amazon RDS), to allow AWS customers to make data easily accessible to their applications or for backup purposes. Storage of sensitive data in the various storage options should consider the technology and accessibility of the data to the Internet to meet CJIS requirements for restricting direct inbound and outbound access to the systems that contain sensitive data.

- For example, Amazon S3 can be configured to encrypt your data at rest with server-side encryption (SSE), Amazon S3 will automatically encrypt your data on write and decrypt your data on retrieval. When Amazon S3 SSE encrypts data at rest, it uses Advanced Encryption Standard (AES) 256-bit symmetric keys. If you choose server-side encryption with Amazon S3, there are several ways to manage the encryption keys.

- AWS Key Management Service (KMS) - a service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses Hardware Security Modules (HSMs) to protect the security of your keys. For customers who use encryption extensively and require strict control of their keys, the AWS Key Management Service provides a convenient management option for creating and administering the keys used to encrypt your data at rest.

- KMS Service Integration – AWS KMS seamlessly integrates with Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon Elastic Transcoder, Amazon WorkMail, and Amazon EMR. This integration means that you can use AWS KMS master encryption keys to encrypt the data you store with these services by simply selecting a check box in the AWS Management Console.

- AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. AWS CloudHSM supports a variety of use cases and applications, such as database encryption, Digital Rights Management (DRM), and Public Key Infrastructure (PKI) including authentication and authorization, document signing, and transaction processing.

Auditing and Accountability

(Ref. CJIS Policy Area 4)

- AWS CloudTrail – AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. AWS CloudTrail logs all user activity within your AWS account. You can see who performed what actions on each of your AWS resources. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

- Amazon CloudWatch - is a monitoring service for AWS cloud resources and the applications you run on AWS. AWS CloudWatch enables you to monitor your AWS resources in near real-time, including Amazon EC2 instances, Amazon EBS volumes, AWS Elastic Load Balancers, and Amazon RDS DB instances.

- AWS Trusted Advisor - provides best practices (or checks) in four categories: **cost optimization, security, fault tolerance, and performance improvement**. For each check, you can review a detailed description of the recommended best practice, a set of alert criteria, guidelines for action, and a list of useful resources on the topic.

- Amazon SNS - can be used to send email or SMS-based notifications to administrative and security staff. Within an AWS account, you can create Amazon SNS topics to which applications and AWS CloudFormation deployments can publish. These push notifications can automatically be sent to individuals or groups within the organization who need to be notified of Amazon CloudWatch alarms, resource deployments, or other activity published by applications to Amazon SNS.

Security by Design – CJIS

Security by Design (SbD) is a security assurance approach that formalizes AWS account design, automates security controls, and streamlines auditing. Instead of relying on auditing security retroactively, SbD provides security control built in throughout the AWS IT management process. By utilizing Security by Design CloudFormation templates, security and compliance in the cloud can be made more efficient and expansive.

SbD encompasses a four-phase approach for security and compliance at scale across multiple industries, standards, and security criteria to include CJIS. AWS SbD can be utilized when designing security and compliance capabilities for all phases of security by allowing the customer to design everything within the AWS customer environment: permissions, logging, trust relationships, encryption enforcement, mandating approved machine images, and more. SbD enables customers to automate the front end structure of an AWS account, reliably coding security and compliance into AWS accounts, making non-compliance of IT controls a thing of the past.

SbD CloudFormation templates, SDKs, IDE Toolkits, and Command Line Tools can be used to support multiple CJIS Policy Areas such as:

- **Policy Area 4**: Auditing and Accountability
- **Policy Area 5**: Access Control
- **Policy Area 6**: Identification and Authentication
- **Policy Area 7**: Configuration Management
- **Policy Area 8**: Media Protection
- **Policy Area 10**: System and Communications Protection and Information Integrity

For more information see: AWS Security by Design or email: aws-securitybydesign@amazon.com

CJIS Security Policy

The following table provides an overview of the CJI Security policy requirements, equivalent NIST controls documented in AWS' FedRAMP System Security Plan (SSP) through the FedRAMP process, a summary of whether the controls are met by AWS alone, met by both AWS and the customer (shared), or is solely a customer responsibility, and details to explain the rationale and provide transparency into AWS' processes in CJIS environments. As a point of clarification a brief description of shared controls is necessary. "**Shared**" controls indicate security requirements, which AWS has addressed within the infrastructure for all components of the system AWS manages (up to the hypervisor/virtualization management layer). It also indicates that those same controls must be addressed by the customer in their environment (from the guest operating system (OS) and on into the customer's systems) apart from those implemented by AWS. Customers with existing CJI workloads and data will typically reuse the majority of their existing compliance documentation when leveraging AWS for CJI.

Within the customer details column there is ***italic*** information which can be used by customer and/or partners to document their implementation details as part of their CJIS Systems Security Plan which can be leveraged to illustrate how the customer or partner meet the intent of the ***Shall*** statements within the CJIS Security Policy.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.1	***Policy Area 1: Information Exchange Agreements*** The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.	N/A	Shared	*[Customer and Partner's use of AWS services should document within existing Governance processes (e.g. security policies, procedures and agreements) the use of AWS services. Additionally, Partners solutions on AWS should establish appropriate information exchange agreements and security recommendations for use of their end customers as it relates to their use AWS customer environments]* References: Security at Scale: Governance in AWS	AWS provides a standard Customer Agreement as well as standardized Rules of Behavior (RoB) between AWS and the customer to allow end users to fully understand AWS' security capabilities as well as the Shared Responsibility model. References: 1. AWS Security Center 2. Intro to Cloud Security 3. AWS Security Resources

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.1.1	***Information Exchange*** Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI. Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document. Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements. There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.	AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12 (2)	Shared	*[Customers and Partners are responsible for establishing information exchange agreements (e.g. CJIS User Agreements) as well as information exchange agreements and security implementation standards which support the CJIS Security Policy Shall statements (e.g. Controls) within 12 policy areas documented within Section 5 Policy & Implementation]* Additionally AWS has created a CJIS Systems Security Plan Template for customers and partners to document their security policy implementation details in preparation for audit and authorization by the sponsoring agency. For more information on how AWS can help document your CJIS security capabilities contact: AWS State & Local Government	AWS has a Control Implementation Summary (CIS) and a Control Tailoring Workbook (CTW) which outlines which controls have been implemented, how they meet requirements within the AWS environment, and whether those controls are inherited from AWS, are shared, or are the customer's sole responsibility. The AWS FedRAMP System Security Plan (SSP) is a comprehensive document, which outlines the controls, parameters, and architecture of the AWS environment. These documents are part of the AWS FedRAMP package that clearly specifies security controls and implementation details. Reference: FedRAMP Compliance in the Cloud

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.1.1.1	***Information Handling*** Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange. The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.	AC-21, CM-9, CP-6, CP-7, IR-8, PL-2, PM-1	Customer	*[Customer and Partners are responsible for creating procedures for handling and storage of information with their use of AWS service.]* Reference: *AWS Data Protection FAQ* AWS information Handling resources: 1. AWS Identity & Access Management (IAM) 2. Encrypting Data at Rest 3. Controlling Access to EC2 Resources 4. Amazon S3 encryption 5. AWS Key Management Service	
5.1.1.2	***State and Federal Agency User Agreements*** Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.	AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12 (2)	Shared	*[The customer* CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) *is responsible for ensuring there is a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs.]*	AWS complies with the FBI's Criminal Justice Information Services (CJIS) standard. We sign CJIS security agreements with our customers; including allowing or performing any required employee background checks according to the **CJIS Security Policy**.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.1.1.3	***Criminal Justice Agency User Agreements*** Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include: 1. Audit. 2. Dissemination. 3. Hit confirmation. 4. Logging. 5. Quality Assurance (QA). 6. Screening (Pre-Employment). 7. Security. 8. Timeliness. 9. Training. 10. Use of the system. 11. Validation.	AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12	Shared	*[The customer and partner are responsible for ensuring Criminal Justice Agency (CJA) receive signed access agreements for personnel with access to CJI as part of their security addendum process]*	To enable this requirement, AWS supports user agreement where applicable, as part of the CJIS security addendum process with our customers, agencies and partners.
5.1.1.4	***Interagency and Management Control Agreements*** A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or inter-agency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an inter-agency agreement. An example of an NCJA (government) is a city information technology (IT) department.	AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12 (2)	Customer	*[The Noncriminal Justice Agency (NCJA) shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA.]*	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.1.1.5	***Private Contractor User Agreements and CJIS Security Addendum*** The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require. Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI. 1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement that specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI,	AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12	Shared	*[The customer and partner are responsible for ensuring Criminal Justice Agency (CJA) receive signed access agreements for personnel with access to CJI as part of their security addendum process]*	To enable this requirement, AWS supports user agreement where applicable, as part of the CJIS security addendum process with our customers, agencies and partners.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7). 2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement that specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).				
5.1.1.6	***Agency User Agreements*** A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board. A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority	AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12 (2	Shared	*[AWS customers and partner should work with the appropriate CJA in order to implement these requirements for the affected user environments built on AWS.]*	AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts pre-employment criminal background checks, as permitted by law, for employees commensurate with their position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank. All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.				
5.1.1.7	***Outsourcing Standards for Channelers*** Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.	PE-3, PS-1, PS-2, PS-3, PS-6, PS-7	Customer	*[The customer and partner are responsible for ensuring Criminal Justice Agency (CJA) receive signed access agreements for personnel with access to CJI as part of their security addendum process]*	By definition AWS is not a direct Channeler; in most cases agencies, customer and partners will have direct access to CJI. AWS supports user agreement background checks where applicable, as part of the CJIS security addendum process with our customers, agencies and partners.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.1.1.8	***Outsourcing Standards for Non-Channelers*** Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.	AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12 (2)	Shared	*[Customers and partners should define the policies that identify functional responsibilities for the administration of logical access and security of the CJI data and implement the requirements of this control.]*	AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts criminal background checks, as permitted by law, for employees and commensurate with the employee's position and level of access.
5.1.2	***Monitoring, Review, and Delivery of Services*** As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.	RA-3, SA-9, SA-9 (1)	Shared	*[Customers and partners can and should maintain overall control and visibility into their environment to include their own vulnerability scanning, pen testing and system monitoring.]* Reference: 1. Acceptable Use Policy 2. Pen testing on AWS 3. Security Bulletins	As part of the FedRAMP process, AWS provides ongoing Continuous Monitoring reports in order to maintain its ATOs. These reports include providing vulnerability scan information, plan of actions and milestones (POA&M), security assessment results to federal agencies that have granted a formal ATO, and other reports which provide assurance that AWS services are being appropriately provided, monitored, and reviewed.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.1.2.1	***Managing Changes to Service Providers*** Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.	RA-3	Shared	*[Customers are responsible for reviewing these notices and understanding which services are applicable to their environment.]* References: 1. Service Health Dashboard 2. AWS Release Notes 3. What’s NEW from AWS	AWS communicates changes to its services through a variety of methods. These may include direct notices to the customer, notices posted to AWS public forums, or changes through the FedRAMP authorization package as part of its ongoing risk management and change management processes.
5.1.3	***Secondary Dissemination*** If CHRI is released to another authorized agency, and that agency was not part of the releasing agency’s primary information exchange agreement(s), the releasing agency shall log such dissemination.	PS-3, PS-6, PS-7	Customer	*[The customer and partners should establishing exchange agreements where applicable.]*	
5.1.4	***Secondary Dissemination of Non-CHRI CJI*** If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.	PS-3, PS-6, PS-7	Customer	*[The customer and partners should establish dissemination and local policy requirements.]*	
5.2	***Policy Area 2: 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. The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.	N/A	Shared	*[Customer and partners should establish basic security awareness training within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.]*	AWS provides annual security awareness training for AWS staff with access to the AWS infrastructure. Where applicable AWS personnel with direct access to CJI shall be required within six months of initial assignment, and biennially thereafter complete a CJIS inclusive security awareness process.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.2.1.1	***All Personnel*** At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI: 1. Rules that describe responsibilities and expected behavior with regard to CJI usage. 2. Implications of noncompliance. 3. Incident response (Points of contact; Individual actions). 4. Media protection. 5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity. 6. Protect information subject to confidentiality concerns — hardcopy through destruction. 7. Proper handling and marking of CJI. 8. Threats, vulnerabilities, and risks associated with handling of CJI. 9. Social engineering. 10. Dissemination and destruction.	AT-2 (2), AT-3	Shared	*[Customer and partner should provide baseline security awareness training for all authorized personnel with access to CJI.]*	AWS is responsible for providing baseline security awareness training for all authorized personnel with access to CJI. Where applicable AWS personnel with direct access to CJI shall be required within six months of initial assignment, and biennially thereafter complete a CJIS inclusive security awareness process.
5.2.1.2	***Personnel with Physical and Logical Access*** 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 both physical and logical access to CJI: 1. Rules that describe responsibilities and expected behavior with regard to information system usage. 2. Password usage and management—including creation, frequency of changes, and protection. 3. Protection from viruses, worms, Trojan horses, and other malicious code. 4. Unknown e-mail/attachments. 5. Web usage—allowed versus prohibited; monitoring of user activity. 6. Spam. 7. Physical Security—increases in risks to systems and data.	AT-2 (2), AT-3, CM-10, PL-4, PL-4 (1)	Shared	*[Customer and partners should ensure personnel with both physical and logical access to CJI receives additional security awareness training relevant to their access.]*	AWS provides comprehensive security training for AWS staff that supports this requirement.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	8. Handheld device security issues—address both physical and wireless security issues. 9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance. 10. Laptop security—address both physical and information security issues. 11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights). 12. Access control issues—address least privilege and separation of duties. 13. Individual accountability—explain what this means in the agency. 14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain. 15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems. 16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. 17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.				

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.2.1.3	***Personnel with Information Technology Roles*** 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 Information Technology personnel (system administrators, security administrators, network administrators, etc.): 1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions. 2. Data backup and storage—centralized or decentralized approach. 3. Timely application of system patches—part of configuration management. 4. Access control measures. 5. Network infrastructure protection measures.	AT-3	Shared	*[Customer and partners should ensure Information Technology personnel (e.g., system administrators, security administrators, network administrators, etc.) receive additional training related to protection from malicious code, data backup and storage, timely implementation of system patches, access control measures and network infrastructure protection measures.]*	AWS's security awareness training addresses all the requirements in the CJIS Security Policy. AWS ensures Information Technology personnel (e.g., system administrators, security administrators, network administrators, etc.) receive additional training related to protection from malicious code, data backup and storage, timely implementation of system patches, access control measures and network infrastructure protection measures.
5.2.2	***Security Training Records*** Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB/Compact Officer. Maintenance of training records can be delegated to the local level.	AT-4, PL-4	Shared	*[Customer and partners should maintaining records of individual basic security awareness training and specific information system security training.]*	AWS maintains training records for AWS employees.
5.3	***Policy Area 3: Incident Response*** There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F	N/A	Shared	*[Customer and partners should extend or create an AWS operational incident handling capability as it relates to for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.]* Reference: Incident response in the cloud	AWS has an established Incident Response (IR) program regarding the detection, investigation, and mitigation of information security-related incidents. Reference: AWS Overview of Security Processes

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.				
5.3.1	***Reporting Information Security Events*** The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.	IR-4 (1), IR-6, IR-6 (1), IR-6 (2), IR-7, IR-7 (1), IR-7 (2), IR-8, PE-17	Shared	*[Customer and partners should establish and/or include their existing incident reporting process for reporting security events to the appropriate authorities as it relates to their AWS customer environments.]*	AWS has an established Incident Response (IR) program regarding the detection, investigation, and mitigation of information security-related incidents. Reference: 1. AWS Vulnerability Reporting
5.3.1.1.1	**FBI CJIS Division Responsibilities** The FBI CJIS Division shall: 1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC). 2. Serve as a central clearing house for all reported intrusion incidents, security alerts, bulletins, and other security-related material. 3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed. 4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips. 5. Track all reported incidents and/or trends. 6. Monitor the resolution of all incidents.	N/A	FBI		Applicable to FBI CJIS Division only.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.3.1.1.2	***CSA ISO Responsibilities*** The CSA ISO shall: 1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response. 2. Identify individuals who are responsible for reporting incidents within their area of responsibility. 3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident. 4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected. 5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area. 6. Act as a single POC for their jurisdictional area for requesting incident response assistance.	N/A	CSA		Applicable to CSA ISO Responsibilities only.
5.3.2	***Management of Information Security Incidents*** A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.	IR-1, IR-8	Shared	*[The AWS shared responsibility model requires you to monitor and manage your environment at the operating system and higher layers.* *Customer and Partners should establish processes for reporting security incidents as they related to their AWS environment as well as options for mitigating security incidents before they occur.]* Reference: AWS Best Practices for DDoS Resiliency	AWS and the customer are responsible for applying a consistent approach to the management of information security incidents. Reference: AWS Vulnerability Reporting

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.3.2.1	***Incident Handling*** The agency shall implement incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.	IR-4, IR-4 (1), IR-4 (3), IR-4 (4), IR-8	Shared	*[Customer and partners should implement an incident handling capability for security incidents which includes preparation, detection and analysis, containment, eradication, and recovery capabilities. There are several AWS services and tools which, can support these capabilities.]* Reference AWS services: - AWS CloudWatch - EC2 Describe API - Amazon Simple Notification Service - AWS Health Dashboard - AWS CloudTrail logs - AWS Config	AWS has an established Incident Response (IR) program regarding the detection, investigation, and mitigation of information security-related incidents. Reference: 1. AWS Vulnerability Reporting
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).	IR-4, IR-4 (1), IR-4 (3), IR-4 (4), IR-8	Shared	*[Customer and partner should establish a responsible process for the collection, retention, and presentation of evidence to conform to the rules for evidence laid down in the relevant jurisdiction(s).]*	AWS has an established Incident Response (IR) program regarding the detection, investigation, and mitigation of information security-related incidents. In order to protect the confidentiality of customer information, AWS does not permit third parties access to data centers. AWS is responsible for working with customer with the collection, retention, and presentation of evidence to conform to the rules for evidence laid down in the relevant jurisdiction(s).
5.3.3	***Incident Response Training*** The agency shall ensure general incident response roles and responsibilities are included as part of required security awareness training.	IR-2, IR-3	Shared	*[Customer and partners should ensure general incident response roles responsibilities are included as part of required security awareness training.]*	AWS includes team roles and responsibilities in its Incident Response program. AWS is responsible for ensuring general incident response roles responsibilities are included as part of required security awareness training.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.3.4	***Incident Monitoring*** The agency shall track and document information system security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.	IR-5	Shared	*[Customer and/or partners should maintaining completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time frame is greater.]*	AWS and the customer are both responsible for tracking and documenting information system security incidents in their respective environments on an ongoing basis.
5.4	***Policy Area 4: Auditing and Accountability*** Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components. Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.	N/A	Shared	*[Customers and partner should define a policy, process for audit and accountability controls managed by the customer. Similar to physical systems, you must implement and maintain logging and monitoring of EC2 instances, applications deployed on EC2 instances, Amazon RDS databases, and any other services part of the AWS customer environment.]* Reference: 1. Auditing Security Checklist for Use of AWS	AWS has implemented a formal audit policy, the "AWS Audit and Accountability Policy" which addresses the roles, responsibilities, and requirements for auditing within the AWS infrastructure.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.4.1	***Auditable Events and Content (Information Systems)*** The agency's information system shall generate audit records for defined events. These defined events include identifying significant events that need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems. The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.	AC-9, AU-2, AU-2 (3), AU-3, AU-3 (1), AU-6, AU-6 (1), AU-6 (3), AU-12, CA-7	Shared	*[Customers and partners should establish audit and accountability controls for their customer environments (e.g. IAM, API and Config access).]* References: 1. Security by Design 2. AWS Security Audit Guideline 3. Amazon Resource Names (ARNs) 4. AWS CloudTrail 5. AWS CloudWatch	AWS has established audit trails to maintain a record of the system activity by system and application processes and by user activity. Specific events are recorded based on a risk assessment that identified auditable event categories.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.4.1.1	***Events*** The following events shall be logged: 1. Successful and unsuccessful system log-on attempts. 2. Successful and unsuccessful attempts to use: a. access permission on a user account, file, directory or other system resource; b. create permission on a user account, file, directory or other system resource; c. write permission on a user account, file, directory or other system resource; d. delete permission on a user account, file, directory or other system resource; e. change permission on a user account, file, directory or other system resource. 3. Successful and unsuccessful attempts to change account passwords. 4. Successful and unsuccessful actions by privileged accounts. 5. Successful and unsuccessful attempts for users to: a. access the audit log file; b. modify the audit log file; c. destroy the audit log file.	AC-9, AU-2, AU-12, CA-7	Shared	*[Customers and partners should implement event logging within their AWS customer environment (e.g. IAM, API calls, Server Access and Load Balancers]* References: 1. Security by Design 2. Logging IAM Events with AWS CloudTrail 3. Server Access Logging S3 4. S3 Bucket logging 5. Access Logs Elastic Load Balancer (ELB)	AWS logs a variety activities in order to support investigations and to meet the AWS Audit and Accountability Policy including: • Successful and unsuccessful account logon events • Account management events • Object access • Policy changes • Privilege functions • Process tracking • System events/error • Administrator activity • Authentication/Authorization checks • Data Deletions, access, changes, and permissions
5.4.1.1.1	***Content*** The following content shall be included with every audited event: 1. Date and time of the event. 2. The component of the information system (e.g., software component, hardware component) where the event occurred. 3. Type of event. 4. User/subject identity. 5. Outcome (success or failure) of the event.	AU-12	Shared	*[Customers and partners should implement content logging using CloudTrail and CloudWatch for operating and application content monitoring]* Reference: 1. Security by Design 2. CloudTrail User Guide 3. Monitor OS & Application Log Files	AWS audited events include date, time, component, type of event, user ID, and outcome for auditable events.
5.4.2	***Response to Audit Processing Failures*** The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit	AU-5, AU-5(2)	Shared	*[Customers and partners should document their policy on how their organization responds to audit processing failures.]* Reference: 1. Security by Design 2. API operations for CloudTrail	Audit processing errors are logged and archived according to the AWS Audit and Accountability Policy.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	storage capacity being reached or exceeded.				
5.4.3	***Audit Monitoring, Analysis, and Reporting*** The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.	AU-6, AU-6 (1), AU-6 (3), AU-7, CA-7	Shared	*[Customers and partners should document their implementation of AWS audit monitoring, analysis, and reporting. There are several capabilities within AWS services as well as partner services such as Splunk AMI]* Reference: 1. Security by Design 2. Web Server Log Analysis 3. Web Log Analysis Architecture 4. Marketplace Log Analysis 5. CloudWatch Log Files	AWS maintains an ongoing audit monitoring, analysis, and reporting posture that investigates and reports suspicious activities and anomalies.
5.4.4	***Time Stamps*** The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.	AU-8, AU-8 (1)	Shared	*[Customers and partners are responsible for configuring time stamps and NTP services on their servers and applications.]* References: 1. Security by Design 2. Setting the Time for Your Linux Instance 3. Setting the Time for a Windows Instance	Timestamps of suit records are generated using internal system clocks that are synchronized to internal Network Time Protocol (NTP) servers. Timestamps are used for log retention, processing, and analysis. All AWS hosts are synced to NTP servers.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
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.	AU-9, AU-9 (4)	Shared	*[Customers and partners are responsible for protecting any logs they generate from their systems as well as the auditing tools themselves.]* References: 1. Security by Design 2. Access Control List (ACL) Overview 3. Managing Access to S3 resources 4. Editing S3 Bucket Permissions	AWS implements several internal processes to help protect audit information and audit tools form unauthorized access, modification, and deletion to include a service for collecting and archiving logs for AWS service owners. This service encrypts logs, protects encryption keys, and uses asymmetric encryption with at least 1024 bits.
5.4.6	***Audit Record Retention*** The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.	AU-4, AU-5 (1), AU-9 (2), AU-11	Shared	*[Customers and partners should establish their record retention policies and technical implementations as applicable. Leading practice for meeting this requirement is setting S3 retentions to 30 days with an archiving rule to move records to Glazier for the remaining 335 days with a delete rule on the 366 day of retention.]* References: 1. Security by Design 2. Archiving S3 to Glazier 3. S3 FAQs	AWS audit logs are stored on an internal AWS service that archives and secures logs stored in S3. All logs are considered "online" and available for the AWS service teams. Audit data is pulled at least every 24 hours.
5.4.7	***Logging NCIC and III Transactions*** A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one-year retention period.	AU-4, AU-11	Customer	*[The customer must establish auditing capabilities to log transactions for one year related to NCIC and III transactions as part of the management of those data sets.]* References: 1. Security by Design 2. Enterprise Splunk Amazon Machine Image (AMI)	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.5	**Policy Area 5: Access Control** Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.	N/A	Shared	*[Customers and provides should configure this capability through the AWS IAM service and the customer's own access management control regime for the customer to address and implement this control.]* References: 1. Amazon IAM documentation	AWS implements this control within the AWS infrastructure
5.5.1	***Account Management*** The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on: 1. Valid need-to-know/need-to-share that is determined by assigned official duties. 2. Satisfaction of all personnel security criteria. The agency responsible for account creation shall be notified when: 1. A user's information system usage or need-to-know or need-to-share changes. 2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.	AC-2, AC-5, IR-8	Shared	*[Customers and partners should create users groups and roles in IAM, and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. The customer can also define which entity is allowed to assume the role. IAM enables organizations with multiple employees to create and manage multiple users under a single AWS account. With IAM policies, it is possible to grant IAM users fine-grained control to AWS services.]* References: 1. Security by Design 2. AWS Identity and Access Management (IAM) 3. AWS IAM Best Practices	AWS User accounts are established as part of the onboarding workflow process in Amazon's Human Resource Management System (HRMS). All employees, vendors, and contractors who require a user account must be on-boarded through Amazon's HR system. As part of the onboarding workflow, the direct manager of the employee, vendor, or contractor requests the establishment of a user account. The approved request serves as the approval to establish a user account

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.5.2	***Access Enforcement*** The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., information system security officers, maintainers, system programmers). Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.	AC-2, AC-2 (1), AC-2 (7), AC-3, AC-3 (3), AC-3 (4), AC-5, AC-6(1), AC-6 (2), AC-12 (1), SC-23 (1), SC-23 (3	Shared	*[The customer and partners can use ACLs to selectively add (grant) certain permissions on individual objects. Amazon S3 Bucket Policies can be used to add or deny permissions across some or all of the objects within a single bucket.* *AWS Identity and Access Management (IAM) enable the customer to create multiple users within the customer's AWS account and manage their permissions via IAM policies. These policies are attached to the users, enabling centralized control of permissions for users under the customer's AWS account. Bucket policies are attached to a bucket and the IAM policies are attached to individual users in the account.]* References: 1. Security by Design 2. S3 Access Control List (ACL) Overview 3. Granting IAM Users Required Permissions	AWS Identity and Access Management (IAM) enables the customer to create multiple users within the customer's AWS account and manage their permissions via IAM policies. These policies are attached to the users, enabling centralized control of permissions for users under the customer's AWS account.
5.5.2.1	***Least Privilege*** The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.	AC-2, AC-2 (4), AC-2 (7), AC-5, AC-6, AC-6 (5), AC-6 (9), AC-10, RA-5 (5)	Shared	*[Customers and partners to grant unique security credentials to every user and specify which AWS service APIs and resources they can access. IAM is secure by default; users have no access to AWS resources until permissions are explicitly granted.]* References: 1. Security by Design 2. AWS IAM Best Practices Blog 3. AWS IAM Best Practices	AWS manages its own infrastructure based on the "least privilege" principal and also implements a variety of segregation of duties designed to ensure that individual access is appropriately limited and restricted.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.				
5.5.2.2	***System Access Control*** Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to: 1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions. 2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.	AC-2, AC-2 (4), AC-2 (7), AC-5, AC-6, AC-6 (5), AC-6 (9), AC-10, RA-5 (5)	Shared	*[Customers and partners should architecting an environment and granting permissions that meet CJI specific access control requirements established by the Agency or local policies.]* References: 1. Security by Design 2. IAM Roles (Delegation and Federation) 3. Managing AWS Access Keys 4. Federated Access to AWS Console	AWS administrators authenticate their SSH connection to the network bastion hosts using an RSA private key and passphrase, then log on to the network device which uses TACACS to authenticate the user with their LDAP user ID and password. For privileged (root) commands, users must escalate privileges using an authenticated password. All escalations of privilege commands are audited.
5.5.2.3	***Access Control Criteria*** Agencies shall control access to CJI based on one or more of the following: 1. Job assignment or function (i.e., the role) of the user seeking access. 2. Physical location. 3. Logical location. 4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside). 5. Time of day and day of week/month restrictions.	AC-2, AC-2 (4), AC-2 (7), AC-5, AC-6, AC-6 (5), AC-6 (9), AC-10, RA-5 (5)	Shared	*[Customers and partners can limiting access to data based on roles, location (i.e., US East, US West), logical location (utilizing Virtual Private Cloud), and network addresses. Time of day and day of week restrictions are normally enforced through federated access controls (i.e., integrating to Windows Active Directory).]* References: 1. Security by Design 2. AWS Security Token Service	AWS has implemented a formal, documented access control policy called "AWS Access Control Policy," System accounts are established by submitting a request using Amazon's self-service system account creation tool. Using this tool, mandatory fields, including unique account name, an account description, account owner, and a justification for the account creation.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.5.2.4	***Access Control Mechanisms*** When setting up access controls, agencies shall use one or more of the following mechanisms: 1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted. 2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices. 3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. 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 5.10.1.2 for encryption requirements). 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.	AC-2, AC-2 (4), AC-2 (7), AC-5, AC-6, AC-6 (5), AC-6 (9), AC-10, RA-5 (5)	Shared	*[Customers and Partners should create unique roles and users accounts for access AWS management console functions, AWS services, as well as instances and data stored within EC2, RDS, S3 or other services.* *In a federated environment, this can be accomplished by assigning unique accounts in the organization's LDAP implementation and only assigning AWS rights to accounts that are individually assigned.]* References: 1. Security by Design 2. AWS Resource-Level Permissions 3. AWS Services integration with IAM 4. Managing Access with ACLs 5. AWS Key Management Service (KMS) 6. Signing AWS API Requests 7. Granting Permissions to AWS Applications	AWS has implemented a formal, documented access control policy called "AWS Access Control Policy," System accounts are established by submitting a request using Amazon's self-service system account creation tool. Using this tool, mandatory fields, including unique account name, an account description, account owner, and a justification for the account creation.
5.5.3	***Unsuccessful Login Attempts*** Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.	AC-7, IA-5 (1)	Shared	*[Customers and partners should configure IAM account settings and MFA to restrict unsuccessful login attempts. In a federated environment, this can be accomplished by assigning unique accounts in the organization's LDAP implementation and only assigning AWS rights to accounts that are individually assigned.]*	AWS administrators access the AWS infrastructure through a combination of methods including SSH using RSA keys with 2,048 bits of strength, bastion hosts, multi-factor tokens, and other mechanisms. Together, these controls exceed the intent of the CJIS policy requirement. Additionally, the customer still has

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
				References: 1. Security by Design 2. Setting an Account Password Policy for IAM Users 3. Multi-Factor Authentication (MFA) Devices with AWS	the option for enforcing this requirement within any internal access management policies (e.g., Windows Active Directory Global Policy Objects).
5.5.4	***System Use Notification*** The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information: 1. The user is accessing a restricted information system. 2. System usage may be monitored, recorded, and subject to audit. 3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties. 4. Use of the system indicates consent to monitoring and recording. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system. Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring,	AC-8, AC-11 (1), AC-22	Shared	*[Customer and partners should create systems use notifications within their hosted applications and specific systems.]* Reference: 1. Security by Design 2. AWS Notification API 3. Amazon Simple Notification Service API 4. Invoking Lambda notification functions	AWS implements a notification banner into the internal management access file, which will appear upon each successful internal remote access request. The banner informs the AWS user that their usage/activities on the systems may be monitored, audited, or recorded as well as sanction.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.				
5.5.5	**Session Lock** The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screensaver with password.	AC-11	Shared	*[Customers and partners should federate their AWS services using AD connector in-order to meet this control for through group policies within Active Directory.]* Reference: 1. Security by Design 2. AWS AD Connector 3. Connecting AD to AWS	AWS implements this control by enforcing client systems (authorized workstations), which are used to remotely access the system, to meet Active Directory sessions lock out requirements through domain policy, which is set to 15 minutes.
5.5.6	***Remote Access*** The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet). The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote	AC-17, AC-17 (3), AC-17 (4), AC-17 (6)	Shared	*[Customers and partners should implement policies and procedures for remote access into their AWS customer environments.* *AWS provides multiple options for securing remote access. Access to the AWS Management Console is logged and monitored by AWS.* *Privileged functions should be configured using Roles verses direct users and in logged using AWS CloudTrail.]*	AWS employs automated mechanisms to facilitate the monitoring and control of remote access methods, through syslog running on the bastion hosts. Auditing occurs on the systems and devices within the sys.log or auth.log files, which are then aggregated and stored for review and incident investigation.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system. Virtual escorting of privileged functions is permitted only when all the following conditions are met: 1. The session shall be monitored at all times by an authorized escort 2. The escort shall be familiar with the system/area in which the work is being performed. 3. The escort shall have the ability to end the session at any time. 4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path. 5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.			Reference: 1. Security by Design 2. Remote Gateway Reference Architecture 3. Connecting Windows EC2 Using RDP 4. Deploy Remote Desktop Gateway on the AWS Cloud 5. AWS Multi-Factor Authentication	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.5.6.1	***Personally Owned Information Systems*** A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.5.7.3 Cellular. This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).	AC-17	Customer	*[Customers and partners should address this requirement with their systems security policies and procedures.]*	Personally owned information systems are prohibited from connecting to the AWS infrastructure.
5.5.6.2	***Publicly Accessible Computers*** Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.	AC-17, AC-22	Customer	*[Customers and partners should address this requirement when accessing their AWS environment through appropriate policies and procedures.]*	
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.	N/A	Customer	*[Customers and partners are responsible for properly identifying and vetting system users prior to granting them access to CJI through appropriate policies and procedures.]*	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.6.1	***Identification Policy and Procedures*** Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.	IA-1, IA-2, IA-2 (5)	Shared	*[The customer and partners can create unique identifiers in IAM; assign them individual security credentials (i.e., access keys, passwords, and Multi-Factor Authentication devices).]* Reference: 1. Security by Design 2. IAM Best Practices 3. IAM Business Use Cases 4. Identities (Users, Groups, and Roles)	AWS uses unique identifiers for all administrators and users with access to the AWS infrastructure. Which operations can be performed by the entity, or AWS service, that assumes the role. The customer can also define which entity is allowed to assume the role.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.6.1.1	***Use of Originating Agency Identifiers in Transactions and Information Exchanges*** An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address. Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency, which is requesting the transaction. Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.	SC-16	Customer	*[Customers and partners are responsible for ensuring that originating agency identifiers (ORIs) are used in each transaction on CJIS systems.]* References: 1. Security by Design 2. Amazon Resource Names (ARNs) and AWS Service Namespaces 3. Monitor AWS ELB Load Balancer 4. ELB Access Logs 5. Enable Access logging	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.6.2	***Authentication Policy and Procedures*** Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy, which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI. Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.	IA-1, IA-2, IA-2 (8), IA-2 (9), IA-3	Shared	*[The customer and partners can create roles in IAM, and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. The customer can also define which entity is allowed to assume the role.]*	AWS has implemented a formal, documented access control policy called "AWS Access Control Policy," System accounts are established by submitting a request using Amazon's self-service system account creation tool. Using this tool, mandatory fields, including unique account name, an account description, account owner, and a justification for the account creation.
5.6.2.1	***Standard Authenticators*** Authenticators are the something you know, something you are, or something you have part of the identification and authentication process. Examples of standard authenticators include passwords, tokens, biometrics, and personal identification numbers (PIN). Agencies shall not allow the same authenticator (i.e., password, PIN) to be used multiple times on a device or system.	IA-5, IA-5(1), IA-5(5), IA-6	Shared	*[Customers must address this requirement through appropriate policies, procedures, and configurations in how they access AWS resources.]* Reference: 1. Security by Design 2. AWS Multi-Factor Authentication 3. AWS Security Token Service 4. Managing Access Keys for IAM Users	AWS does not re-use the same authenticators across multiple systems. Where practical, AWS has implemented unique multi-factor authentication such as electronic key fobs, soft certificates, asymmetric encryption, and passwords.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.6.2.1 .1	***Password*** Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall: 1. Be a minimum length of eight (8) characters on all systems. 2. Not be a dictionary word or proper name. 3. Not be the same as the User ID. 4. Expire within a maximum of 90 calendar days. 5. Not be identical to the previous ten (10) passwords. 6. Not be transmitted in the clear outside the secure location. 7. Not be displayed when entered.	IA-5, IA-5 (1), IA-5 (4)	Shared	*[Customers and partners are responsible for controlling the creation of user accounts. AWS IAM features include basic password management options for local accounts such as password length and complexity requirements. Customers and partners should establish a policy for the servers that align with the applicable CJIS requirements.]* Reference: 1. Security by Design 2. Managing AWS account passwords 3. Setting an Account Password Policy for IAM Users	AWS administrators employ the Password Tool to associate an RSA public key with their system account. This public key is propagated to all hosts in the host classes that the user has permissions to manage. This allows the administrator to SSH to the hosts with their user id and the RSA private key, which the user maintains, protected by a passphrase. AWS enforces password complexity in the AWS LDAP with the AWS Password tool, which is employed by users to change passwords.
5.6.2.2	***Advanced Authentication*** Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions. When user-based certificates are used for authentication purposes, they shall: 1. Be specific to an individual user and not to a particular device. 2. Prohibit multiple users from utilizing the same certificate. 3. Require the user to "activate" that certificate for each use in some manner (e.g., passphrase or user-	IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (11), IA-2 (13), IA-3 (1), IA-5(2), IA-5 (11), MA-4, SC-37, SC-37 (1)	Shared	*[Customers and partners can use Multi-factor authentication (MFA) for extra security (Advanced Authentication) for privileged IAM roles (roles should be used for access to sensitive resources).]* References: 1. Security by Design 2. Using Multi-Factor Authentication (MFA) in AWS 3. AWS Developer Authenticated Identities	AWS administrators authenticate their SSH connection to the network bastion hosts using an RSA private key and passphrase, then log on to the network device which uses TACACS to authenticate the user with their LDAP user ID and password. For privileged (root) commands, users must escalate privileges using an authenticated password. All escalations of privilege commands are audited.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	specific PIN).				
5.6.2.2.1	***Advanced Authentication Policy and Rationale*** The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect. The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token). 1. CSO approved compensating controls to meet the AA requirement on agency-issued smartphones, tablets, and iPads are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required	IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (11), IA-3 (1), IA-5 (2), IA-5(11), MA-4	Customer	*[Customers and partners are responsible for determining when Advanced Authentication must be used in establishing an appropriate policy and rationale.]* References: 1. Security by Design 2. Managing Federation in AWS 3. External Identity Providers 4. Amazon Cognito Identity 5. Adding a Hardware Virtual Private Gateway to Your VPC 6. AWS VPN CloudHub	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. The compensating controls shall: Meet the intent of the CJIS Security Policy AA requirement 2. Provide a similar level of protection or security as the original AA requirement 3. Not rely upon the existing requirements for AA as compensating controls Mobile Device Management (MDM) must be implemented and provide at least two of the other examples of compensating controls listed below. Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls. The proposed compensating controls for AA are a combination of controls that provide acceptable assurance it is the authorized user authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.				

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.6.2.2.2	***Advanced Authentication Decision Tree*** The following AA Decision Tree, coupled with figures 9 and 10 below, assist decision makers in determining whether or not AA is required. 1. Can request's originating location be determined physically? If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2. a. The IP address is attributed to a physical structure; or b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure. If neither (a) or (b) above are true then the answer is "no". Skip to question number 4. 2. Does request originate from within a physically secure location (that is not a police vehicle) as described in Section 5.9.1? If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3. a. The IP address is attributed to a physically secure location; or b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location. If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required. 3. Are all required technical controls implemented at this location or at the controlling agency? If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement waived. a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network	IA-2 (1), IA-2 (2), IA 2(3), IA-2 (4), IA-2 (11), IA-3 (1), IA-5 (2), IA-5 (11), MA-4	Customer	*[Customers and Partners are responsible for creating an Advanced Authentication Decision tree based on their specific implementation of AWS.]* References: 1. Security by Design 2. Managing Federation in AWS 3. External Identity Providers 4. Amazon Cognito Identity 5. Adding a Hardware Virtual Private Gateway to Your VPC 6. AWS VPN CloudHub	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10. If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required. 4. Does request originate from an agency-managed user device? If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 5. a. The static IP address or MAC address can be traced to registered device; or b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices. If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required. 5. Is the agency managed user device associated with and located within a criminal justice conveyance? If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to question 6. a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or b. The certificate presented is associated with a device associated with a criminal justice conveyance; or c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance. If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7. 6. Has there been an acquisition or upgrade since 2005? If any of the (a), (b), (c), or (d) statements below are true the answer to the above question is “yes”. Proceed to question				

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	number 7. a. The "green-screen" MDTs have been replaced with laptops or other mobile devices; or b. An upgrade of technology exceeding 25% of the cost of the system being upgraded has taken place; or c. Any upgrade to the system encryption module has taken place; or d. Any upgrade to the system that is not replacing like technology has taken place. If none of the (a), (b), (c), or (d) statements above are true then the answer is "no". Decision tree completed. AA requirement waived. 7. Was IPSec implemented to meet the requirements of Policy Version 4.5? If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement is waived. a. The budget acquisition of IPSec was completed prior to January 1, 2009 and IPSec was subsequently implemented; or b. Implementation of IPSec was completed prior to January 1, 2009. If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.				
5.6.3	***Identifier and Authenticator Management*** The agency shall establish identifier and authenticator management processes.	IA-4, IA-4 (2), IA-4 (4), IA-5, IA-5 (8), IA-8	Customer	*[The customer and/or partner should establish identifier and authenticator management processes.]* References: 1. Security by Design	
5.6.3.1	***Identifier Management*** In order to manage user identifiers, agencies shall: 1. Uniquely identify each user. 2. Verify the identity of each user. 3. Receive authorization to issue a user identifier from an appropriate agency official.	AC-2 (3), IA-4, IA-4 (2), IA-4 (4), IA-5 (3), IA-5 (8), IA-8	Shared	*[Customers and partners are responsible for managing their own user identities and permissions according to this requirement.]* References: 1. Security by Design	All access to the AWS infrastructure from AWS administrators is unique and requires verification.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	4. Issue the user identifier to the intended party. 5. Disable the user identifier after a specified period of inactivity. 6. Archive user identifiers.				
5.6.3.2	***Authenticator Management*** In order to manage information system authenticators, agencies shall: 1. Define initial authenticator content. 2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators. 3. Change default authenticators upon information system installation. 4. Change/refresh authenticators periodically. Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.	IA-5, IA-5 (6), IA-5 (8)	Customer	*[Customer and/or partner are responsibility based on customer agency requirements.]* References: 1. Security by Design 2. AWS IAM Services 3. Signing and Authenticating REST API Requests 4. Amazon Cognito 5. AWS Security Token Service	
5.6.4	***Assertions*** Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be: 1. Digitally signed by a trusted entity (e.g., the identity provider). 2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.	IA-2 (12), IA-8 (1), IA-8 (2), IA-8 (3)	Shared	*[Customer and partners should leverage identity certificates within various AWS services such as IAM, ELB and CloudFront to ensure trust of identities within their AWS customer environment.]* References: 1. Security by Design 2. Working with Server Certificates 3. SSL Certificates for Elastic Load Balancing 4. Install and Configure OpenSSL	AWS utilizes a combination of internal and trusted external certification authorities for validating individual identities. X.509 certificates are issued internally through a self-service certificate creation tool signed by the Amazon.com IT Security Certificate Authority. For external access points, commercial CA's are used. Private keys and certificates are stored and distributed securely.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.				
5.7.1	***Access Restrictions for Changes*** Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.	CM-3, CM-3 (2), CM-4, CM-4 (2), CM-5 (5), CM-5 (6), CM-6, CM-9, MA-2, MA-5, SA-10	Shared	*[Customers and partners should establish their own CM Plan for their systems within AWS.]* References: 1. Security by Design 2. AWS Config Guide 3. ITIL Event Management in the Cloud	AWS has a Change Management (CM) plan which governs the process to making significant changes to hardware, software, or firmware. The CM Plan is designed to make changes without disrupting users, and the vast majority of changes are made with no impact to the customers.
5.7.1.1	***Least Functionality*** The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.	CM-2, CM-3, CM-6, CM-7, CM-7 (1), CM-7 (2), CM-7 (3), CM-7 (4), CM-7 (5), CM-8 (3), CM-10, CM-11, SA-4 (9), SA-9(2)	Shared	*[Customers and partners should configure their AWS application, service, or operating system to provide only essential capabilities; based on least functionality principals.]* References: 1. Security by Design 2. Adhere to IAM Best Practices	The AWS infrastructure was designed with least functionality principals. Customers must likewise configure their own applications and services with least functionality.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.7.1.2	***Network Diagram*** The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams. The network topological drawing shall include the following: 1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point. 2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient. 3. "For Official Use Only" (FOUO) markings. 4. The agency name and date (day, month, and year) drawing was created or updated.	CA-3, CA-9, SC-7 (4)	Customer	*[Customers and partners should create their own network diagrams for their AWS environments according to the parameters in this control.]* References: 1. Security by Design 2. AWS Architecture Center 3. AWS Icons for Architecture Diagrams	
5.7.2	***Security of Configuration Documentation*** The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.	CM-2, CM-5, CM-5 (1), CM-5 (2), CM-8, CM-8 (1), CM-9, SA-5	Shared	*[Customers and partners should incorporate protective measures for system documentation.]* References: 1. Security by Design	AWS protects its security configuration and shares the documentation only with those that have a validated need to know, and only for a limited time. AWS shares information with the federal government and protects documentation through additional controls such as Adobe LiveCycle services.
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. Procedures shall be defined for securely handling, transporting and storing media.	N/A	Shared	*[Customers and partners should address this control within their environment via appropriate policies and procedures.]* References: 1. Security by Design	AWS has implemented a formal "Media Protection Policy" which outlines the requirements for protecting electronic media.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.8.1	***Media Storage and Access*** The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.	AC-20 (2), CP-6, CP-7, MA-3 (3), MP-2, MP-3, MP-4	AWS		AWS has implemented a formal "Media Protection Policy" which outlines the requirements for protecting electronic media. AWS restricts access to digital media within their data centers through the implementation of physical and environmental security controls.
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.	MP-5	AWS		AWS has implemented a formal "Media Protection Policy" which outlines the requirements for protecting electronic media. Customers must address this control within their environment via appropriate policies and procedures. Magnetic, non-magnetic, and hardcopy media types are not transported outside of the customer environments.
5.8.2.1	***Electronic Media in Transit*** "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in 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 other controls to ensure the security of the data.	MP-5, MP-5 (4)	Shared	*[Customers and partners should develop polices and procedures related to their CJI media transfers.]* References: 1. Security by Design 2. AWS Key Management Service	AWS has implemented a formal "Media Protection Policy" which outlines the requirements for protecting electronic media. Customers must address this control within their environment via appropriate policies and procedures. Magnetic, non-magnetic, and hardcopy media types are not transported outside of the customer environments.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.8.2.2	***Physical Media in Transit*** The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.	MP-5	Customer	*[Customers and partners should address this control within their environment via appropriate policies and procedures.]*	
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. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.	MA-2, MP-6, MP-6(1), MP-6(2), MP-6(3)	AWS		AWS has established a Data Destruction Policy, Data Destruction Guidelines, and Media Protection Policy. Portable magnetic media, non-magnetic media, and paper output are not permitted or applicable to the AWS environment. For other data storage services (such as standard hard drives), AWS follows its Media Destruction Procedures.
5.8.4	***Disposal of Physical Media*** Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.	MP-6	AWS		AWS has established a Data Destruction Policy, Data Destruction Guidelines, and Media Protection Policy. Portable magnetic media, non-magnetic media, and paper output are not permitted or applicable to the AWS environment. For other data storage services (such as standard hard drives), AWS follows its Media Destruction Procedures.
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.	N/A	Shared	*[Customers and partners are responsible for establishing their own Policies that address their own physical and environmental policies.]*	AWS has established a "Physical and Environment Protection Policy" which establishes requirements. The Data Center Operations Portal contains additional procedures related to the engineering, design, and operations of data center physical security and environmental protection.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
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. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.		Shared	*[Customers and partners are responsible for any applicable security perimeter requirements for their facilities.]*	AWS maintains strong controls around its data centers. Access to AWS data centers is limited to a small number of AWS employees, and AWS customers are prohibited from entering AWS data centers. Entry areas are the only publically accessible areas of data centers, where non-permanent personnel check-in and are validated as authorized personnel and issued appropriate access cards. Intrusions detection systems and other technologies are used to protect and sound alarms if the security perimeter is breached. .
5.9.1.2	***Physical Access Authorizations*** The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.	MA-4(7), MA-5, PE-2, PE-2(1)	Shared	*[Customers and partners must implement a process to control secure locations in accordance with this control.]*	AWS maintains a list of authorized personnel with access to the AWS data centers.
5.9.1.3	***Physical Access Control*** The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.	PE-3, PE-3(3)	AWS		Only authorized personnel are allowed to enter the AWS data centers. Every access is individually verified prior to granting access.
5.9.1.4	***Access Control for Transmission Medium*** The agency shall control physical access to information system distribution and transmission lines within the physically secure location.	PE-4	AWS		AWS maintains control over physical access to distribution and transmissions lines.
5.9.1.5	***Access Control for Display Medium*** The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.	PE-5	Customer	*[This is a customer and/or partner responsibility. AWS systems do not display CJI information.]*	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
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.	PE-3, PE-5, PE-6, PE-6 (1)	AWS		Access to AWS data centers is monitored by trained guards 24x7, video surveillance, and intrusion detection systems.
5.9.1.7	***Visitor Control*** The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.	PE-2 (3), PE-3	AWS		Visitors are not authorized into AWS facilities.
5.9.1.8	***Delivery and Removal*** The agency shall authorize and control information system-related items entering and exiting the physically secure location.	PE-8	AWS		All equipment entering or existing AWS data centers must be approved prior to their introduction or removal. Data storage components are always destroyed before leaving AWS data centers.
5.9.2	***Controlled Area*** If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum: 1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI. 2. Lock the area, room, or storage container when unattended. 3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view. 4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.	PE-2, PE-5	AWS		AWS meets all requirements defined for a "physically secure location".

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.10	***Policy Area 10: System and Communications Protection and Information Integrity*** Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.	SC-1, SC-7, SC-7(1), SC-7(2), SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(12), SC-7(13), SC-7(18)	Shared	*[Customers and partners should also address this control within the systems operated on AWS as well as within their physical infrastructure.]* References: 1. Security by Design 2. AWS Elastic Load Balancers 3. Security Groups for Your Load Balancer	Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the AWS network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.
5.10.1	***Information Flow Enforcement*** The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are: 1. Prevent CJI from being transmitted unencrypted across the public network. 2. Block outside traffic that claims to be from within the agency. 3. Do not pass any web requests to the public network that are not from the internal web proxy. Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.	AC-4, AC-20, AC-20(1), CA-3, CA-9, IA-5(7), SC-7(4), SC-7(8), SC-7(11), SC-10, SC-15, SC-15(1)	Shared	*[Customers and partners should define and manage their own ACLs, NCLs and VPC's.]* References: 1. Security by Design 2. AWS Network and Security 3. Security Groups for VPCs 4. Network ACLs 5. Adding Hardware Virtual Private Gateway to VPC	AWS Security approved ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic within the AWS infrastructure.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.10.1.1	***Boundary Protection*** The agency shall: 1. Control access to networks processing CJI. 2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. 3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls. 4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use. 5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open"). 6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.	AC-20, CA-3 (1), CA-3 (2), CA-3 (5), PE-3(2), SC-5, SC-5(1), SC-5(2), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-24	Shared	*[To support customers and partners with FIPS 140- 2 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL- terminating load balancers in AWS GovCloud (US) operate using FIPS 140- 2 Level 2 validated hardware.}* References: 1. Security by Design 2. VPC Endpoints 3. AWS GovCloud Endpoints	AWS has strategically placed a limited, but growing, number of access points to AWS. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows the customer to establish a secure communication session with their storage or compute instances within AWS. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet- facing edge of the AWS network. These connections each have dedicated network devices.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.10.1.2	***Encryption*** 1. Encryption shall be a minimum of 128 bits. 2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption). EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2.3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption). 4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards. Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete. Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard, which certifies the packaging of an implementation. 5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall: a) Include authorization by a supervisor or a responsible official. b) Be accomplished by a secure process that verifies the identity of the certificate holder. c) Ensure the certificate is issued to the intended party.	AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-17, SC-28, SC-28(1), SI-7(6)	Shared	*[Customer and partners can choose to connect to AWS through multiple secure protocols. AWS supports the use of the Secure Shell (SSH) network protocol to enable the customer to connect remotely to their UNIX/Linux. Customers and partners can also connect remotely to their Windows instances using Remote Desktop Protocol (RDP) by utilizing an RDP certificate generated for their instance.]* Note: AWS requires that every message be authenticated. For API requests using SOAP, messages must be hashed and signed for integrity and non- repudiation. AWS services require that SOAP messages be secured using the WS- Security standard Binary Security Token profile, consisting of an X.509 certificate with an RSA public key. References: 1. Security by Design 2. Elastic Load Balancing 3. Overview of Security Processes	AWS protects the confidentiality of transmitted data through the use of symmetric encryption of data before transmission to ensure the message contents are not readable in transit. SSL or TLS session are terminates at load balancers or, for S3 connections, at the web servers. Both the load balancers and the web servers employ OpenSSL. Cryptographic ciphers available: AES-256-CBC, AES-128-CBC, 3DES-EDE-CBC

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.10.1.3	***Intrusion Detection Tools and Techniques*** The agency shall implement network-based and/or host-based intrusion detection tools. The CSA/SIB shall, in addition: 1. Monitor inbound and outbound communications for unusual or unauthorized activities. 2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort. 3. Employ automated tools to support near real-time analysis of events in support of detecting system level attacks.	SC-7 (19), SI-4, SI-4 (1), SI-4 (2), SI-4 (4), SI-4 (5), SI-4 (7), SI-4 (9), SI-4 (11), SI-4 (12), SI-7, SI-7 (1), SI-7 (7)	Shared	*[Customers and partners are responsible to deploy requisite intrusion detection solutions in the data environment.]* References: 1. Security by Design 2. Intrusion Detection in the Cloud	AWS security monitoring tools are in position to identify several types of system anomalies for the AWS infrastructure. If issues are identified, the AWS incident response process is initiated. Additionally, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of service degradation.
5.10.1.4	***Voice over Internet Protocol*** Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors. In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI: 1. Establish usage restrictions and implementation guidance for VoIP technologies. 2. Change the default administrative password on the IP phones and VoIP switches. 3. Utilize Virtual Local Area Network	SC-19	Customer	*[VoIP is not applicable to the AWS environment. The customer and/or partner should address this control as applicable.]*	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	(VLAN) technologies to segment VoIP traffic from data traffic. Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.				
5.10.1.5	***Cloud Computing*** Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy. The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.	N/A	AWS		AWS is a FedRAMP Moderate compliant Cloud Service Provider and meets NIST guidelines for secure cloud hosting.
5.10.2	***Facsimile Transmission of CJI*** CJI transmitted via facsimile is exempt from encryption requirements.	N/A	AWS		Facsimile is not applicable in the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.10.3	***Partitioning and Virtualization*** As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization existed previously, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.	SC-2, SC-4	Shared	*[Customer and partners can isolate their environment in their own virtual network and connect to their existing IT infrastructure using industry-standard encrypted IPSec VPN and direct connect to their Virtual Private Cloud (VPC). AWS recommends that customers further protect their data using appropriate means. One common solution is to run an encrypted file system on top of the virtualized disk device.]* References: 1. Security by Design 2. Amazon Virtual Private Cloud 3. Expanding a Linux Partition 4. Linux AMI Virtualization Types	AWS utilizes a highly customized hypervisor, taking advantage of paravirtualization. Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional security separation between the two. **Note:** Customer instances have no access to raw disk devices, but instead are presented with virtualized disks that map logical blocks to physical blocks on the disk device.
5.10.3.1	***Partitioning*** The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality. The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following: 1. Different computers. 2. Different central processing units. 3. Different instances of the operating system. 4. Different network addresses. 5. Other methods approved by the FBI CJIS ISO.	SC-2, SC-2 (1), SC-3, SC-4, SC-32	Shared	Customer and partner have a variety of ways to meet partitioning requirements in the AWS infrastructure. This may include the use of physical separation through separate services (GovCloud versus US East/West), Dedicated Instances, Availability Zones, Regions, or logical controls such as the use of Virtual Private Clouds (VPC's), Access Control Lists (ACLs), encryption and key management, or access control. References: 1. Security by Design 2. AWS Regions and Endpoints 3. VPC Endpoint for Amazon S3 4. Access Control List (ACL) Overview	Traffic that is not explicitly allowed to or from an instance is automatically denied. In addition to security groups, network traffic entering and exiting each subnet can be allowed or denied via network Access Control Lists (ACLs).

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.10.3.2	***Virtualization*** Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment: 1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc. 2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment. 3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally. 4. Device drivers that are "critical" shall be contained within a separate guest. The following are additional technical security control best practices and should be implemented wherever feasible: 1. Encrypt network traffic between the virtual machine and host. 2. Implement IDS and IPS monitoring within the virtual machine environment. 3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact. 4. Segregate the administrative duties for the host. Appendix G-1 provides some reference and additional background information on virtualization.	SC-2, SC-4	Shared	*[Customer and partner instances have no access to raw disk devices, but instead are presented with virtualized disks that map logical blocks to physical blocks on the disk device. Customer and partners should review the different options for setting their EC2 instances and machine images.]* References: 1. Security by Design 2. Amazon EC2 3. Amazon Machine Images (AMI) 4. AMI Types	AWS utilizes a highly customized hypervisor, taking advantage of paravirtualization. Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional security separation between the two.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.10.4.1	***Patch Management*** The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as: 1. Testing of appropriate patches before installation. 2. Rollback capabilities when installing patches, updates, etc. 3. Automatic updates without individual user intervention. 4. Centralized patch management. Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.	CM-3, CM-4, CM-4 (1), RA-5, RA-5 (1), RA-5 (2), RA-5 (3), SA-11, SA-11 (1), SI-2, SI-2 (2), SI-2 (3)	Shared	*[Customers and partners should track and implement patch management processes on their AWS systems.]* References: 1. Security by Design 2. Amazon Machine Images (AMI) 3. AWS Windows AMI Version History 4. Updating Instance Software	All AWS patch management activities must go through the patch validation/vetting process by the service team responsible for researching vulnerabilities. Patches are applied after the security and infrastructure teams have reviewed the risks, implementation, fixes, and potential impact.
5.10.4.2	***Malicious Code Protection*** The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available). The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and	MA-3 (2), SI-3, SI-3 (1), SI-3 (2)	Shared	*[Customers and Partners should define a malicious code protection approach for their use of AWS services.]* References: 1. Security by Design 2. AWS Overview of Security Services 3. AV protection AWS marketplace	The AWS infrastructure is built primarily on a customized Linux-based environment. AWS has taken a non-traditional approach to malicious code protection, and uses a combination of internal research, open source community-distributed software alerts, and has special support contracts to receive appropriate notifications when a security alert is released (and in some cases before it is made public). AWS deploys changes using its approved change management process.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	information systems and resident scanning is employed.				
5.10.4.3	***Spam and Spyware Protection*** The agency shall implement spam and spyware protection. The agency shall: 1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote access servers). 2. Employ spyware protection at workstations, servers and mobile computing devices on the network. 3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.	SI-8, SI-8 (1), SI-8 (2)	Shared	*[Customers and partners are responsible for detecting and preventing spam and spyware on their AWS systems and services they deploy.]* References: 1. Security by Design 2. AWS Overview of Security Services 3. Spam & Spyware protection on AWS marketplace	AWS has limited exposure to spam and spyware in its infrastructure environment, which is not connected to e-mail servers and is heavily Linux based. Malware mitigation practices are in place across the infrastructure.
5.10.4.4	***Security Alerts and Advisories*** The agency shall: 1. Receive information system security alerts/advisories on a regular basis. 2. Issue alerts/advisories to appropriate personnel. 3. Document the types of actions to be taken in response to security alerts/advisories. 4. Take appropriate actions in response. 5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	SI-5, SI-5 (1), SI-11	Shared	*[Customers and partner should define a process for receiving and issuing system security alerts within their environment.]* References: 1. AWS Security Bulletins 2. Security Resources	AWS uses a combination of internal research, open source community-distributed software alerts, and special support contracts to receive appropriate notifications when a security alert is released (in some cases before it is made public).
5.10.4.5	***Information Input Restrictions*** The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only. Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	SI-10, SI-12	Customer	*[The customer and partners are responsible for restricting the information input to any connection to FBI CJIS services to authorized personnel only.]*	

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.11	***Policy Area 11: Formal Audits*** Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.	N/A	Shared	*[The customers and partners are responsible for conducting formal audits to ensure compliance with applicable statutes, regulations and policies.]* References: 1. AWS Published Certifications	Amazon Web Services Cloud Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of **AWS cloud infrastructure**, compliance responsibilities will be **shared**. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS **Compliance enablers** build on traditional programs; helping customers to establish and operate in an AWS security control environment.
5.11.1.1	***Triennial Compliance Audits by the FBI CJIS Division*** The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	N/A	Shared	*[The customer and/or partners are responsible for supporting FBI CJIS Division audits and in turn requesting support from AWS if applicable.]*	AWS is a FedRAMP compliant CSP. The Veris Group, LLC, assessed AWS. An accredited FedRAMP 3PAO and has been granted two Agency FedRAMP Authorizations by the US Department of Health and Human Services (HHS) after demonstrating compliance with the FedRAMP security requirements.
5.11.1.2	***Triennial Security Audits by the FBI CJIS Division*** The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be	CA-2	Shared	*[The customer and/or partners are responsible for supporting FBI CJIS Division audits and in turn requesting support from AWS if applicable.]*	AWS is a FedRAMP compliant CSP. The Veris Group, LLC, assessed AWS. an accredited FedRAMP 3PAO and has been granted two Agency FedRAMP Authorizations by the US Department of Health and Human Services (HHS) after demonstrating compliance with the FedRAMP security requirements.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.				
5.11.2	***Audits by the CSA*** Each CSA shall: 1. At a minimum, triennially audit all CJAs and NCJAs, which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies. 2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies. 3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	CA-2	Shared	*[The customer and/or partners are responsible for supporting FBI CJIS Division audits and in turn requesting support from AWS if applicable.]*	AWS is a FedRAMP compliant CSP. The Veris Group, LLC, assessed AWS. An accredited FedRAMP 3PAO and has been granted two Agency FedRAMP Authorizations by the US Department of Health and Human Services (HHS) after demonstrating compliance with the FedRAMP security requirements.
5.11.3	***Special Security Inquiries and Audits*** All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.	CA-2, CA-2 (1), CA-5, CA-6, CA-7 (1), CM-3 (4)	Shared	*[The customer and/or partners are responsible for supporting FBI CJIS Division audits and in turn requesting support from AWS if applicable.]*	AWS is a FedRAMP compliant CSP. The Veris Group, LLC, assessed AWS. an accredited FedRAMP 3PAO and has been granted two Agency FedRAMP Authorizations by the US Department of Health and Human Services (HHS) after demonstrating compliance with the FedRAMP security requirements.
5.12	***Policy Area 12: Personnel Security*** Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.	N/A	Shared	*[Customers and partners are responsible for establishing their own personnel security policies.]*	AWS has implemented a formal, documented personnel security policy called "AWS Personnel Security Policy," that is updated and reviewed annually. The AWS Personnel Security Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.12.1.1	***Minimum Screening Requirements for Individuals Requiring Access to CJI:*** 1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with: (i) 5 CFR 731.106; and/or (ii) Office of Personnel Management policy, regulations, and guidance; and/or (iii) agency policy, regulations, and guidance. (See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check. 2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency. 3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority 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.	PS-2, PS-3, PS-3 (1), PS-3 (2), PS-3 (3), PS-6, PS-6 (2), PS-7	Shared	*[Customers and partner should address this control within their AWS environment through appropriate policies, procedures and implementations.]*	AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and commensurate with the employee's position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate. 5. 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. 6. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction. 7. 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. 8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial. 9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times. It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.				

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.12.1.2	***Personnel Screening for Contractors and Vendors*** In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements: 1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. 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. 2. If a record of any kind is found, 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-appointed Security Officer. 3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter. 4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified. 5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants. 6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not	PS-2, PS-3, PS-7	Shared	*[Customers and partners should ensure contractors' identification is verified via the state of residency and national fingerprint-based record check.]*	AWS has addressed this control with documented policies and procedures.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	warrant disqualification. The CGA may request the CSO to review a denial-of-access determination.				
5.12.2	***Personnel Termination*** The agency, upon termination of individual employment, shall immediately terminate access to CJI.	PS-4	Shared	*[Customers and partners should also address this control within their AWS environment through appropriate policies and procedures.]*	Accounts are reviewed every 90 days and explicit re- approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems. Requests for changes in access are captured in the Amazon permissions management tool audit log. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked.
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.	PS-5	Shared	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	Accounts are reviewed every 90 days and explicit re- approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems. Requests for changes in access are captured in the Amazon permissions management tool audit log. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked.
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.	PS-8	Shared	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	AWS has established sanctions, including termination, for personnel that violate AWS policies. Customers are responsible for creating their own sanctions for their systems and employees.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.13	***Mobile Devices*** The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections – without requiring network or peripheral cabling. Annex G of the Security Policy provides reference material and additional information on mobile devices. Examples of wireless technologies include, but are not limited to: 802.11x, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.	N/A	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	There are no wireless access points allowed within the system boundaries. Wireless access is not permitted within the AWS infrastructure.
5.13.1.1	***All 802.11x Wireless Protocols*** Agencies shall: 1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture. 2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices. 3. Place APs in secured areas to prevent unauthorized physical access and user manipulation. 4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes. 5. Enable user authentication and encryption mechanisms for the management interface of the AP.	AC-18, SI-4 (14), SI-4 (15)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	There are no wireless access points allowed within the system boundaries. Wireless access is not permitted within the AWS infrastructure.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1. 7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized. 8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services. 9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features. 10. Ensure that encryption key sizes are at least 128 bits and the default shared keys are replaced by unique keys. 11. Ensure that the ad hoc mode has been disabled. 12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption. 13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly. 14. Segregate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs. 15. When disposing of access points that will no longer be used by the agency, clear				

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	access point configuration to prevent disclosure of network configuration, keys, passwords, etc.				
5.13.1.2	***Cellular*** Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks. Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include: 1. Loss, theft, or disposal. 2. Unauthorized access. 3. Malware. 4. Spam. 5. Electronic eavesdropping. 6. Electronic tracking (threat to security of data and safety of the criminal justice professional). 7. Cloning (not as prevalent with later generation cellular technologies). 8. Server-resident data.	AC-19, AC-19 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	There are no cellular devices allowed within the system boundary. Cellular devices are not permitted to connect to the AWS infrastructure.
5.13.1.2.1	***Cellular Service Abroad*** Certain functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider, which is considered a "trusted" entity by the device. When devices are authorized for use 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.	AC-19, AC-19 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	There are no cellular devices allowed within the system boundary. Cellular devices are not permitted to connect to the AWS infrastructure.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
5.13.1.2.2	***Voice Transmissions Over Cellular Devices*** Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.	AC-19, AC-19 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	VoIP is not applicable to the AWS environment.
5.13.1.3	***Bluetooth*** Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices. Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial-of-service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target know vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.	AC-18 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	Bluetooth is not applicable to the AWS environment. Customers must address this requirement through appropriate policies and procedures according to the agency's operational and business processes.
5.13.2	***Mobile Device Management (MDM)*** MDM facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery (if so desired by the agency). Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and application coupled with device specific technical policy can provide a robust method for device configuration	AC-19, AC-19 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	management if properly implemented. Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. Agencies shall implement the following controls when allowing CJI access from cell/smart phones and tablet devices: 1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device. 2. MDM with centralized administration configured and implemented to perform at least the: i. Remote locking of device ii. Remote wiping of device iii. Setting and locking device configuration iv. Detection of "rooted" and "jailbroken" devices v. Enforce folder or disk level encryption vi. Application of mandatory policy settings on the device vii. Detection of unauthorized configurations or software/applications				
5.13.3	***Wireless Device Risk Mitigations*** Organizations shall, at a minimum, ensure that cellular wireless devices: 1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1 2. Are configured for local device authentication (see Section 5.13.9.1). 3. Use advanced authentication. 4. Encrypt all CJI resident on the device. 5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated. 6. Employ personal firewalls or run a	AC-19, AC-19 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level. 7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.				
5.13.3.1	***Legacy 802.11 Protocols*** Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.	AC-18 (5), SI-4 (15)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	There are no wireless access points allowed within the system boundaries. Wireless access is not permitted within the AWS infrastructure.
5.13.4	***System Integrity*** Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third-party MDM, application, or supporting service infrastructure.	CM-1, CM-2, CM-2 (1), CM-2 (3), CM-2 (7), CM-3, CM-3 (1), CM-3 (2)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.
5.13.4.1	***Patching/Updates*** Based on the varying connection methods for mobile devices, an "always on" connection cannot be guaranteed for patching and updating. Devices without "always on" cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching. Agencies shall monitor mobile devices not capable of an "always on" cellular connection (i.e. Wi-Fi only or Wi-Fi with cellular on-demand) to ensure their patch and update state is current.	CM-3, CM-4, CM-4 (1), RA-5, RA-5 (1), RA-5 (2), RA-5 (3), SA-11, SA-11 (1), SI-2, SI-2 (2), SI-2 (3)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.
5.13.4.2	***Malicious Code Protection*** Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central	MA-3 (2), SI-3, SI-3 (1), SI-3 (2)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device. Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. An appropriately configured MDM shall be used on smartphones and tablets to prevent the installation of unauthorized software or applications.				
5.13.4.3	***Physical Protection*** Due to small form factors and the fact that mobile devices are often stored in lower security areas, the risk to theft or loss of the device and any data stored on it is elevated. Physical protections will often be the responsibility of the assigned device user. When mobile devices are authorized for use to access CJI are lost or stolen, agencies shall: 1. Have the ability to determine the location of agency controlled smartphones and tablets. 2. Immediately wipe the device.	AC-19, PE-18, PE-18 (1), PE-20	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.
5.13.4.4	***Personal Firewall*** For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities: 1. Manage program access to the Internet. 2. Block unsolicited requests to connect	SC-18, SC-18 (1), SC-18 (2), SC-18 (3), SC-18 (4)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	to the user device. 3. Filter incoming traffic by IP address or protocol. 4. Filter incoming traffic by destination ports. 5. Maintain an IP traffic log. Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform similar functions a personal firewall would provide on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.				
5.13.5	***Incident Response*** In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. Special reporting procedures for mobile devices shall apply in any of the following situations: 1. Loss of device control. 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.	IR-1, IR-2, IR-4, IR-8	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	a. CJI stored on device b. Lock state of device c. Capabilities for remote tracking or wiping of device 3. Device compromise. 4. Device loss or compromise outside the United States.				
5.13.6	***Auditing and Accountability*** The ability to implement audit and accountability functions may not be natively included on mobile devices with limited function operating systems (e.g. Android, Apple iOS). Either additional device management systems or auditing from systems accessed by the mobile device may be necessary to ensure appropriate levels of auditing exist. Additionally, the type of connectivity capable by the device will also affect the ability to collect audit logs for review. A mobile device not capable of providing required audit and accountability on its own accord shall be monitored by a MDM, other management system, or application capable of collecting required log data.	AU-1, AU-2, AU-4, AU-6, AU-6 (1), AU-6 (3), AU-7, AU-11, CA-7, CM-8, CM-8 (1)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.
5.13.7	***Access Control*** Multiple user accounts are not generally supported on limited function mobile operating systems. This may mean the policy requirements for access control (Section 5.5 Access Control, regarding account management) would not apply to the operating system, but rather to a particular application, either stand-alone to the device or as part of a client server architecture.	AC-5, AC-6, AC-6 (5), AC-6 (9), AC-19, AC-19 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.
5.13.8	***Wireless Hotspot Capability*** Many mobile devices include the capability to function as a wireless access point or Wi-Fi hotspot that allows other devices to connect through the device to the Internet over the devices cellular network.	AC-18, AC-18 (1), SC-40, SI-4 (15)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	When an agency allows mobile devices to function as a wireless access point, they shall be configured: 1. In accordance with the requirements in section 5.13.1.1 All 802.11 Wireless Protocols 2. To only allow connections from agency authorized devices				
5.13.9	***Identification and Authentication*** Due to the technical methods used for identification and authentication on many limited feature mobile operating systems, achieving compliance may require many different components.	A-1, IA-2, IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (8), IA-2 (9), IA-2 (11), IA-3, IA-5 (2), IA-5 (11), MA-4, SC-37, SC-37 (1)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment..
5.13.9.1	***Local Device Authentication*** When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.	IA-1, IA-2, IA-2 (5)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment. Customers must address this requirement through appropriate policies and procedures.
5.13.10	***Device Certificates*** Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user. When certificates or cryptographic keys used to authenticate a mobile device are stored on the device, they shall be: 1. Protected against being extracted from the device 2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access	AC-19, IA-3, IA-3 (4)	Customer	*[Customers and partners should address this control within their AWS environment through appropriate policies and procedures.]*	MDM is not applicable to the AWS environment.

CJIS Policy	Requirement	NIST 800-53rev4 Control Mapping	Responsibility	Customer or Partner Recommendations	AWS Details
	attempts 3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use.				

Further Reading

AWS Resources

- AWS Compliance Center: http://aws.amazon.com/compliance
- AWS Security by Design: https://aws.amazon.com/compliance/security-by-design/
- Introduction to Auditing the Use of AWS: https://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf
- AWS Security Center: http://aws.amazon.com/security
- AWS Security Resources: http://aws.amazon.com/security/security-resources
- FedRAMP FAQ: http://aws.amazon.com/compliance/fedramp-faqs/
- Risk and Compliance Whitepaper: http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
- Cloud Architecture Best Practices Whitepaper: http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf
- AWS Products Overview: http://aws.amazon.com/products/
- AWS Sales and Business Development: http://aws.amazon.com/compliance/contact/public-sector/