CJIS Security Policy Template

(This document is part of the CJIS Workbook package, which also includes CJIS Security Policy Requirements, CJIS Security Policy Workbook, and the Criminal Justice Information Service Compliance on AWS whitepaper.)

March 2017

amazon webservices

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

Introduction

The CJIS Security Policy (Security Policy) outlines a minimum set of security requirements that create security controls for managing and maintaining Criminal Justice Information (CJI). The CJIS Advisory Policy Board (APB) manages the policy with national oversight from the CJIS division of the FBI. Unlike FedRAMP, there is no centralized adjudication body for determining what is or isn't compliant with the Security Policy. As a result, vendors/cloud service providers (CSPs) that want to provide CJIS compliant solutions to multiple law enforcement agencies may have to gain formal CJIS authorizations from each of the state/local jurisdictions that they support. For more information, see the CJIS Compliance page.

The CJIS Security Policy Template, delivered as part of the CJIS Workbook package, describes the shared responsibility model between AWS and customers when working to achieve a CJIS compliant environment. Customers can use this information as a template for documenting the implementation of applicable CJIS requirements. The template also outlines AWS's response on the shared responsibility controls, which can be submitted to an authorizing agency as part of a customer's CJIS solution.

This template, and AWS's approach to helping support a CJIS compliant environment have been favorably reviewed by the CJIS APB subcommittee, various state-level CJIS authorizing agencies and AWS partners.

The CJIS Workbook package also contains the CJIS Security Policy Workbook Excel spreadsheet, which consolidates all of the information provided by the CJIS Security Policy Template and CJIS Security Policy Requirements documents into a single format.

Responsibilities

After evaluating the 13 Policy Areas and 131 security requirements defined in the CJIS Security Policy, AWS has determined that 10 controls can be directly inherited from AWS; 78 controls represent a shared responsibility between AWS and the customer, and 43 controls are solely the responsibility of the customer. The following table describes how these responsibilities are reflected in the CJIS security policy table.

Control Responsibility	Customer Responsibility Cell	AWS Responsibility Cell
Shared	Information to help the customer meet their responsibility.	A description of how AWS meets its responsibility.
Customer only	Information to help the customer meet their responsibility.	N/A
AWS only	N/A	A description of how AWS meets its responsibility.

“Shared” controls indicate security requirements that AWS has addressed at the infrastructure level for components that are within AWS’s management responsibility (i.e., infrastructure up to the hypervisor/virtualization management layer). It also indicates controls that customers must address in their environment (from the guest operating system (OS) to the customer’s systems). If you have existing CJI workloads and data, you will typically reuse the majority of your existing compliance documentation.

The CJIS Security Policy Template

The following table contains space for customers to map CJIS Systems Security Plan implementation details. For a complete description of each requirement, as well as relevant FedRAMP controls, see CJIS Security Policy Requirements.

> ***Note:*** *You can replace the* ***italic*** *text in the* ***Customer Details*** *column with your CJIS Systems Security Plan implementation details.*

Table 1: Using the CJIS security policy

Requirement	Customer Responsibility	AWS Responsibility
5.1 – Policy Area 1: Information Exchange Agreements	*[Customer's and agencies' use of AWS services should be documented within existing governance processes (e.g. security policies, procedures and agreements) governing the use of AWS services.]*	AWS identifies standardized Rules of Behavior (RoB) between AWS and the customer to allow end users to fully understand AWS's security capabilities as well as the Shared Responsibility model. References: • AWS Security Center • Intro to Cloud Security • AWS Security Resources

5.1.1 – Information Exchange	*[Customers (or their partners) may need to establish a CJIS information exchange agreement with CJIS authorizing agencies that include the 12 Security Policy areas documented within Section 5 Policy & Implementation]*	AWS has a Control Implementation Summary (CIS) and a Control Tailoring Workbook (CTW) outlining the controls that have been implemented, how they meet requirements within the AWS environment, whether those controls are inherited from AWS, and whether the controls are shared or are the customer's sole responsibility. The AWS FedRAMP System Security Plan (SSP) is a comprehensive document that explains the controls, parameters and architecture of the AWS environment. These documents are a part of the AWS FedRAMP package that clearly specifies security controls and implementation details. Reference: • FedRAMP Compliance in the Cloud
5.1.1.1 – Information Handling	*[Customers (or their partners) are responsible for properly protecting sensitive data stored on AWS.*	N/A

5.1.1.2 – State and Federal Agency User Agreements	*[The CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) are responsible for ensuring there are appropriate signed written user agreements with the FBI CJIS Division.]*	N/A
5.1.1.3 – Criminal Justice Agency User Agreements	*[Customers (or their partners) are responsible for ensuring Criminal Justice Agency (CJA) receive signed access agreements, as appropriate, for personnel with access to CJI as part of their security addendum process]*	To enable this requirement, AWS supports user agreements, where applicable, in accordance with the CJIS Security Policy and CJIS Security Policy Workbook.
5.1.1.4 – Interagency and Management Control Agreements	*[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 remain solely with the CJA.]*	N/A
5.1.1.5 – Private Contractor User Agreements and CJIS Security Addendum	*[Customers (or their partners) are responsible for ensuring the 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 agreements, where applicable, in accordance with the CJIS Security Policy and CJIS Security Policy Workbook.

5.1.1.6 – Agency User Agreements	*[Customers (or their partners) should work with the appropriate CJA in order to implement these requirements for the affected user environments built on AWS.]*	AWS is not considered a Non-Criminal Justice Agency as it does not access CJI directly or implement systems that connect to CJI. AWS services are consumed by Criminal Justice Agency and Non-Criminal Justice Agency entities for the purposes of their systems to connect to CJI. AWS will comply with the CJIS Security Policy in providing fingerprints from its covered administrators for the purposes of performing background checks under Security Agreements with customers.
5.1.1.7 – Outsourcing Standards for Channelers	*[Customers (or their partners) 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]*	AWS is not a direct “Channeler” because it does not build or implement the CJI system or otherwise access CJI. As such, the requirement does not apply to AWS.

5.1.1.8 – Outsourcing Standards for Non-Channelers	*[Customers (or their 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 is not a "Contractor" because it does not build or implement the CJI system or otherwise access CJI. As such, the requirement does not apply to AWS.
5.1.2 – Monitoring, Review, and Delivery of Services	*[Customers (or their partners) can and should maintain overall control and visibility into their environment to include their own vulnerability scanning, pen testing and system monitoring.]*	AWS provides monthly continuous monitoring reporting to FedRAMP. These reports include vulnerability scans, plan of actions and milestones (POA&M), and additional information such as expected changes upcoming, new services etc.
5.1.2.1 – Managing Changes to Service Providers	*[Customers (or their partners) are responsible for reviewing these notices and understanding which services are applicable to their environment.]*	AWS communicates changes to its services through a variety of methods. These may include notices to customers in accordance with the AWS customer agreement (aws.amazon.com/agreement), notices posted to AWS public forums, or changes through the monthly continuous monitoring reporting to FedRAMP.

5.1.3 – Secondary Dissemination	*[Customers (or their partners) should establish exchange agreements where applicable.]*	N/A
5.1.4 – Secondary Dissemination of Non-CHRI CJI	*[Customers (or their partners) should establish dissemination and local policy requirements.]*	N/A
5.2 – Policy Area 2: Security Awareness Training	*[Customers (or their 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, covered AWS personnel with access to CJI shall be required within six months of initial assignment, and biennially thereafter, to complete a CJIS inclusive security awareness process training.
5.2.1 Awareness Topics	*N/A*	N/A

5.2.1.1 – Level One Security Awareness Training	*[Customers (or their partners) should provide baseline security awareness training for all authorized personnel with access to CJI.]*	AWS has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. AWS has developed, documented and disseminated role based security awareness training for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. Training includes, but is not limited to the following information and includes the listed topics in the CJIS Policy requirement (when relevant to the employee's role): • Workforce conduct standards • Candidate background screening procedures • Clear desk policy and procedures • Social engineering, phishing, and malware • Data handling and protection • Compliance commitments • Security precautions while traveling • How to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel

		• How to recognize suspicious communications and anomalous behavior in organizational information systems • Practical exercises that reinforce training objectives
5.2.1.2 – Level Two Security Awareness Training	*[Customers (or their partners) should ensure personnel with both physical and logical access to CJI receive additional security awareness training relevant to their access.]*	AWS has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. AWS has developed, documented and disseminated role based security awareness training for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. Training includes, but is not limited to the following information includes the listed topics in the CJIS Policy requirement and (when relevant to the employee's role): • Workforce conduct standards • Candidate background screening procedures • Clear desk policy and procedures

		• Social engineering, phishing, and malware • Data handling and protection • Compliance commitments • Security precautions while traveling • How to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel • How to recognize suspicious communications and anomalous behavior in organizational information systems • Practical exercises that reinforce training objectives • ITAR responsibilities
5.2.1.3 – Level Three Security Awareness Training	*[Customers (or their 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 has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. AWS has developed, documented and disseminated role based security awareness training for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. Training includes, but is not limited to the following information and

		includes the listed topics in the CJIS Policy requirement (when relevant to the employee's role): • Workforce conduct standards • Candidate background screening procedures • Clear desk policy and procedures • Social engineering, phishing, and malware • Data handling and protection • Compliance commitments • Security precautions while traveling • How to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel • How to recognize suspicious communications and anomalous behavior in organizational information systems • Practical exercises that reinforce training objectives • ITAR responsibilities
5.2.1.4 – Level Four Security Awareness Training	*[Customers (or their 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 has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. AWS has developed, documented and disseminated role based security awareness training for personnel

		responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. Training includes, but is not limited to the following information and includes the listed topics in the CJIS Policy requirement (when relevant to the employee’s role): • Workforce conduct standards • Candidate background screening procedures • Clear desk policy and procedures • Social engineering, phishing, and malware • Data handling and protection • Compliance commitments • Security precautions while traveling • How to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel • How to recognize suspicious communications and anomalous behavior in organizational information systems • Practical exercises that reinforce training objectives
5.2.2 – Security Training Records	*[Customers (or their partners) should maintain records of individual basic security awareness training and specific information system security training.]*	AWS maintains training records for AWS employees in accordance with the CJIS Security Policy requirements.

5.3 – Policy Area 3: Incident Response	*[The customer is responsible for developing an IR plan, as well as conducting training and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the system.*	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
5.3.1 – Reporting Information Security Events	*[The customer is responsible for developing an IR plan, as well as conducting training and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the system.]*	AWS has an established Incident Response (IR) program regarding the detection, investigation, and mitigation of information security-related incidents. Reference: • AWS Vulnerability Reporting
5.3.1.1 – FBI CJIS Division Responsibilities	*N/A*	N/A

5.3.1.2 – CSA ISO Responsibilities	*N/A*	N/A
5.3.2 – Management of Information Security Incidents	*[The AWS shared responsibility model requires that customers monitor and manage their environments at the operating system and higher layers. The customer is responsible for developing an IR plan, as well as conducting training and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the system.*	AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. Events originate from several sources such as: o Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers. o Trouble tickets entered by an AWS employee. o Calls to the 24x7x365 technical support hotline. o If the event meets incident criteria, the relevant on-call support engineer use Event Management Tool system to start an

		engagement and page relevant program resolvers (for example, Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause. 2. Recovery Phase - The relevant resolvers will perform break fix to address the incident. After addressing troubleshooting, break fix and affected components, the call leader will assign follow-up documentation and follow-up actions and end the call engagement. 3. Reconstitution Phase – The call leader will declare the recovery phase complete after the relevant fix activities have been addressed. The post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and actions, such as design changes, will be captured in a Correction of Errors (COE) document and tracked to completion. To ensure the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing provides excellent coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the Amazon Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities. The Incident Response Test Plan is executed annually, in conjunction with the Incident Response plan. The test plan includes multiple scenarios, potential vectors of attack, the inclusion of the systems integrator in reporting and coordination (when applicable), as well as varying

		reporting/detection avenues (i.e. customer reporting/detecting, AWS reporting/detecting). AWS Incident Management planning, testing and test results are reviewed by third party auditors.
5.3.2.1 – Incident Handling	*[Customers (or their partners) should implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery capabilities. There are several AWS services and tools that can support these capabilities.]*	AWS employees are trained on how to recognize suspected security incidents and where to report them. When appropriate, incidents are reported to relevant authorities. AWS maintains the AWS security bulletin webpage, located at https://aws.amazon.com/security/security-bulletins, to notify customers of security and privacy events affecting AWS services. Customers can subscribe to the Security Bulletin RSS Feed to keep abreast of security announcements on the Security Bulletin webpage. The customer support team maintains a Service Health Dashboard webpage, located at http://status.aws.amazon.com/, to alert customers to any broadly impacting availability issues. The customer is responsible for reporting incidents involving customer storage, virtual machines, and applications, unless the incident is caused by AWS. For more information refer to the AWS Vulnerability Reporting webpage: https://aws.amazon.com/security/vulnerability-reporting/.

5.3.2.2 – Collection of Evidence	*[Customers (or their partners) should establish a responsible process for the collection, retention, and presentation of evidence that conforms to the rules for evidence laid down in the relevant jurisdiction(s).]*	AWS will work with customers (or law enforcement officials) in the collection, retention, and presentation of evidence that conforms to the rules for evidence laid down in the relevant jurisdiction(s).
5.3.3 – Incident Response Training	*[Customers (or their partners) should ensure general incident response roles and 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 identifying general incident response roles and responsibilities as part of required security awareness training.
5.3.4 – Incident Monitoring	*[Customer (or their partners) should 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.]*	AWS requires that the Security and/or affected Service team conduct a post-mortem to determine the cause of incident, as well as to document lessons-learned. AWS employs several automated mechanisms to support incident response and handling requirements, including online reporting and communication tools, a trouble ticketing system, and an incident tracking database.

5.4 – Policy Area 4: Auditing and Accountability	*[Customers (or their partners) 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 Amazon Elastic Compute Cloud (EC2) instances, applications deployed on Amazon EC2 instances, Amazon Relational Database Service (Amazon RDS) databases, and any other services part of the AWS customer environment.]*	AWS has implemented a formal audit policy, which addresses the roles, responsibilities, and requirements for auditing within the AWS infrastructure.
5.4.1 – Auditable Events and Content (Information Systems)	*[Customers (or their partners) are responsible for identifying the appropriate audit events that will be implemented within their AWS account. Customers are responsible turning on CloudTrail, as well as properly configuring auditable events on any operating systems they install on EC2, and applications hosted on their EC2 instances.]*	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 identifies auditable event categories.
5.4.1.1 – Events	*[Customers (or their partners) are responsible for reviewing audit logs generated by their AWS account via CloudTrail, as well as logs generated by their EC2 instances and any applications hosted on EC2. Customers can use CloudWatch Logs as a centralized means of analyzing their audit logs generated by CloudTrail and by their EC2 instances).]*	AWS logs a variety of activities in order to support investigations and to meet the AWS Audit and Accountability Policy. These activities include: • 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
5.4.1.2 – Content	*[Customers (or their partners) are responsible for reviewing audit logs generated by their AWS account via CloudTrail, as well as logs generated by their EC2 instances and any applications hosted on EC2. Customers can use CloudWatch Logs as a centralized means of analyzing their audit logs generated by CloudTrail and by their EC2 instances.]*	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	*[Customers (or their partners) are responsible for configuring alarms or notifications on their EC2 instances in order to notify administrators of audit log failures within the customer's EC2 instances. Customer administrators are responsible for responding to audit failures within their EC2 instances.]*	Audit processing errors are logged and archived according to AWS policy.

5.4.3 – Audit Monitoring, Analysis, and Reporting	*[Customers (or their partners) are responsible for reviewing audit logs generated by their AWS account via CloudTrail, as well as logs generated by their EC2 instances and any applications hosted on EC2. Customers can use CloudWatch Logs as a centralized means of analyzing their audit logs generated by CloudTrail and by their EC2 instances.]*	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: • Port scanning attacks • Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) • Application performance metrics • Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged and the logs are retained for at least 90 days, including relevant access request information, such as the data accessor IP address, object, and operation. All requests to AWS KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request, under which Customer Master Key (CMK), and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account.

5.4.4 – Time Stamps	*[Customers (or their partners) are responsible for configuring their EC2 instances to synchronize with the ntp servers required by their organization.]*	The information systems use internal system clocks synchronized to Network Time Protocol to generate time stamps for audit records. Third party testing of AWS' clock synchronization validates that system configurations are automatically provisioned to NTP time.
5.4.5 – Protection of Audit Information	*[Customers (or their partners) are responsible for properly protecting audit data generated by their EC2 instances and by CloudTrail. Customers can protect their audit data through the proper implementation of encryption at rest, as well as through implementation of access policies to restrict access to audit data to authorized users.]*	AWS implements processes to help protect audit information and audit tools from unauthorized access, modification, and deletion. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available to authorized users for inspection or analysis on demand, and in response to security-related or business-impacting events.
5.4.6 – Audit Record Retention	*[Customers (or their partners) are responsible for storing their audit logs on S3 or Amazon Glacier in order to preserve them for the period required by their organization.]*	AWS audit logs are stored on an internal AWS service that archives and secures logs stored in Amazon 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	*[Customers (or their partners) must establish auditing capabilities to log NCIC and III transactions for one year as part of the management of those data sets.]*	N/A
5.5 – Policy Area 5: Access Control	*[Customers (or their partners) should configure access control using the IAM service and their own access management control regime.]*	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. Access control procedures are systematically enforced through proprietary tools. Procedures exist so that Amazon employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a periodic basis. In addition, password complexity settings for user authentication to AWS systems are managed in compliance with Amazon's Corporate Password Policy. AWS has established formal policies and procedures to delineate standards for logical access to AWS platform and infrastructure hosts. Where permitted by law, AWS requires that all employees undergo a background investigation commensurate with their position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

5.5.1 – Account Management	*[Customers (or their partners) should create user 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.]*	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
5.5.2 – Access Enforcement	*[Customers (or their partners) can use access control lists (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.* *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. Bucket policies are attached to a bucket and the IAM policies are attached to individual users in the account.]*	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	*[Customers (or their partners) can grant unique security credentials to every user and specify that 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.]*	AWS implements least privilege and also implements a variety of segregation of duties designed to limit and restrict individual access. Customers are responsible for managing their own accounts and permissions leveraging the aforementioned IAM capabilities as well as any other policies and procedures within their non-AWS environment.

5.5.2.2 – System Access Control	*[Customers (or their partners) should architect an environment and grant permissions that meet CJI specific access control requirements as established by the Agency or local policies.]*	Privileged access to AWS systems are allocated based on least privilege, approved by an authorized individual prior to access provisioning, and assigned a different user ID than used for normal business use. Duties and areas of responsibility (for example, access request and approval, change management request and approval, change development, testing and deployment, etc.) are segregated across different individuals to reduce opportunities for an unauthorized or unintentional modification or misuse of AWS systems. Customers retain the ability to manage segregations of duties of their AWS resources.
5.5.2.3 – Access Control Criteria	*[Customers (or their partners) are responsible for properly configuring their AWS account to restrict access to all security-relevant functions and information, as well as any of their AWS applications that are not to be available to the public.]*	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. Access control procedures are systematically enforced through proprietary tools.
5.5.2.4 – Access Control Mechanisms	*[Customers (or their partners) can and should create unique user accounts to access AWS management console functions, AWS services, as well as instances and data stored within Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Simple Storage Service (Amazon 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.]*	Procedures exist so that Amazon employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a periodic basis. In addition, password complexity settings for user authentication to AWS systems are managed in compliance with Amazon’s Corporate Password Policy. AWS has established formal policies and procedures to delineate standards for logical access to AWS platform and infrastructure hosts. Where permitted by law, AWS requires that all employees undergo a background investigation commensurate with their position and level of access. The

		policies also identify functional responsibilities for the administration of logical access and security.
5.5.3 – Unsuccessful Login Attempts	*[IAM does not currently support locking out of accounts due to failed logon attempts. Customers can implement account lockout through federation to their existing AD/LDAP, or mitigate the risk through the use of multi-factor authentication.]*	AWS controls access to systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. Remote access requires multi-factor authentication and the number of unsuccessful log-on attempts is limited. All remote administrative access attempts are logged, and the logs are reviewed by the Security team for unauthorized attempts or suspicious activity. If suspicious activity is detected, the incident response procedures are initiated.
5.5.4 – System Use Notification	*[Customers (or their partners) should create system use notifications within their hosted applications and specific systems.]*	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 possible sanctions.

5.5.5 – Session Lock	*[Customers (or their partners) are responsible for configuring appropriate session lock controls on the customer's EC2 instances. Customers can federate access with their internal LDAP/AD to enforce session lock rules.]*	AWS has implemented a session lock out policy that is systematically enforced. The session lock is retained until established identification and authentication procedures are performed.
5.5.6 – Remote Access	*[Customers (or their partners) are responsible for documenting and implementing remote access from their network to their AWS applications.]*	AWS requires multi-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations. Remote access to AWS production environments is limited to defined security groups. The addition of members into a group must be reviewed and approved by authorized individuals who confirm the user's need for access to the environment. Baselining of groups (e.g., reviewing of existing members in the group for their continued need for access) occurs every 90 days by the manager and is enforced by the permissions tool which provides automated notification to the manager.
5.5.6.1 – Personally Owned Information Systems	*[Customers (or their 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	*[Customers (or their partners) should address this requirement when accessing their AWS environment using appropriate policies and procedures.]*	Publically accessible computers are not used to provide the AWS infrastructure Services.
5.6 – Policy Area 6: Identification and Authentication	*[Customers (or their partners) are responsible for properly identifying and vetting system users prior to granting them access to CJI through appropriate policies and procedures.]*	All employees, vendors, and contractors who require a user account must be on-boarded through Amazon's HR management 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.
5.6.1 – Identification Policy and Procedures	*[Customers (or their partners) are responsible for establishing an Identification and Authentication Policy for their AWS systems, and for properly configuring their root AWS account, IAM accounts and EC2 instances in accordance with their policies and procedures. Customers can leverage AWS' federation capabilities in order to use their existing enterprise identity and authentication servicer (LDAP/AD) within their AWS account.]*	AWS uses unique identifiers for all administrators and users that have access to the AWS infrastructure to track and determine 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.

5.6.1.1 – Use of Originating Agency Identifiers in Transactions and Information Exchanges	*[Customers (or their partners) are responsible for ensuring that originating agency identifiers (ORIs) are used in each transaction on CJIS systems.]*	N/A
5.6.2 – Authentication Policy and Procedures	*[Customers (or their partners) can create roles in Identity and Access Management (IAM), and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. Customers 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 include unique account name, account description, account owner, and a justification for the account creation.
5.6.2.1 – Standard Authenticators	*[Customers (or their partners) must address this requirement using appropriate policies, procedures, and configurations in how they access AWS resources.]*	AWS implements multi-factor authentication such as electronic key fobs, soft certificates, asymmetric encryption, and passwords.

5.6.2.1.1 – Password	*[Customers (or their partners) are responsible for controlling the creation of user accounts. Identification and Access Management (IAM) features include basic password management options for local accounts such as password length and complexity requirements. Customers (or their partners) should establish a policy for the servers that align with the applicable CJIS requirements.]*	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. Access control procedures are systematically enforced through proprietary tools. Procedures exist so that Amazon employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a periodic basis. In addition, password complexity settings for user authentication to AWS systems are managed in compliance with Amazon's Corporate Password Policy. AWS has established formal policies and procedures to delineate standards for logical access to AWS platform and infrastructure hosts. Where permitted by law, AWS requires that all employees undergo a background investigation commensurate with their position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.
5.6.2.1.2 – Personal Identification Number	*[Customers (or their partners) are responsible for controlling the creation of user accounts. IAM features include basic password management options for local accounts such as password length and complexity requirements. Customers (or their partners) should establish a policy for the servers that align with the applicable CJIS requirements.]*	N/A

5.6.2.2 – Advanced Authentication	*[Customers (or their partners) can use Multi-factor authentication (MFA) to provide extra security (Advanced Authentication) to privileged IAM users (users who are allowed access to sensitive resources).]*	Amazon personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate Amazon credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.
5.6.2.2.1 – Advanced Authentication Policy and Rationale	*[Customers (or their partners) are responsible for determining when Advanced Authentication must be used in establishing an appropriate policy and rationale.]*	N/A
5.6.2.2.2 – Advanced Authentication Decision Tree	*[Customers (or their partners) are responsible for creating an Advanced Authentication Decision tree based on their specific implementation of AWS.]*	N/A

5.6.3 – Identifier and Authenticator Management	*[Customers (or their partners) should establish identifier and authenticator management processes.]*	N/A
5.6.3.1 – Identifier Management	*[Customers (or their partners) are responsible for managing their own user identities and permissions according to this requirement.]*	AWS personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate Amazon credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.
5.6.3.2 – Authenticator Management	*[Customers (or their partners) are responsible based on customer agency requirements.]*	N/A

5.6.4 – Assertions	*[Customers (or their partners) should leverage identity certificates within various AWS services such as IAM, Elastic Load Balancing, and Amazon CloudFront to ensure trust of identities within their AWS customer environment.]*	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 (CA). For external access points, commercial CA's are used. Private keys and certificates are stored and distributed securely.
5.7 – Policy Area 7: Configuration Management		
5.7.1 – Access Restrictions for Changes	*[For all Change Management controls, customers (or their partners) are responsible for properly implementing configuration management, to include maintaining a baseline configuration and change control of their systems deployed on AWS.]*	AWS Service teams maintain service specific change management standards that are inherited and built on the AWS Change Management guidelines. AWS applies a systematic approach to managing change to ensure that all changes to a production environment are reviewed, tested, and approved. The AWS Change Management approach requires that the following steps be complete before a change is deployed to the production environment: 1. Document and communicate the change via the appropriate AWS change management tool. 2. Plan implementation of the change and rollback procedures to minimize disruption.

		3. Test the change in a logically segregated, non-production environment. 4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review. 5. Attain approval for the change by an authorized individual. In order to validate that changes follow the standard change management procedures, all changes to the AWS production environment are reviewed on at least a monthly. An audit trail of the changes is maintained for a least a year. Emergency changes follow the AWS incident response procedures. Exceptions to the change management processes are documented and escalated to AWS management.
5.7.1.1 – Least Functionality	*[Customers (or their partners) should configure their AWS application, service, or operating system to provide only essential capabilities; based on least functionality principles.]*	The AWS infrastructure was designed with least functionality principles. Customers must likewise configure their own applications and services with least functionality.

5.7.1.2 – Network Diagram	*[Customers (or their partners) should create their own network diagrams for their AWS environments according to the parameters in this control.]*	N/A
5.7.2 – Security of Configuration Documentation	*[Customers (or their partners) should incorporate protective measures for system documentation.]*	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.
5.8 – Policy Area 8: Media Protection	*[Customers (or their partners) should address this control within their environment via appropriate policies and procedures.]*	AWS has implemented a formal Media Protection Policy that outlines the requirements for protecting electronic media.

5.8.1 – Media Storage and Access	*N/A*	AWS restricts access to data centers through the implementation of physical and environmental security controls. All personnel granted access to AWS Data Center facilities (via a badge swipe and PIN combination) are screened against a pre-authorized list of those needing access in order to perform their duties or are fully escorted, as appropriate. All personnel working at GovCloud data centers MUST be US persons.
5.8.2 – Media Transport	*N/A*	AWS does not allow any media outside the datacenters
5.8.2.1 – Digital Media in Transit	*[Customers (or their partners) should develop policies and procedures related to their CJI media transfers.]*	AWS does not transport any media containing CJI. Removable or portable magnetic, non-magnetic, and hardcopy media types are not used to store data, so they are not transported outside of the system boundary.

5.8.2.2 – Physical Media in Transit	*[Customers (or their partners) should address this control within their environment via appropriate policies and procedures.]*	AWS does not sanitize physical media, as the AWS system does not provide services that render printed or physical media.
5.8.3 – Digital Media Sanitization and Disposal	*N/A*	AWS sanitizes all forms of digital media, regardless if it is removable storage or non-removable storage. • Cryptographic Wipe • Firmware "Secure Erase" Command Destroy methods include: • Shredding • Incineration • Degaussing • Crushing AWS employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. Since it is presumed that in the media lifecycle that the data will at some point hold sensitive customer or AWS data, all media is treated as sensitive or Controlled Unclassified Information (CUI). This subsequently enforces that all media be rendered unreadable and destroyed at the end of lifecycle, when compromised, or malfunctioning. The Data Destruction Procedures were developed in accordance to NSA Media Destruction Guidance, NIST Media Sanitization Standards (NIST SP 800-88).

5.8.4 – Disposal of Physical Media	*N/A*	AWS does not sanitize physical media, as it does not provide services that render printed media.
5.9 – Policy Area 9: Physical Protection	*[Customers (or their partners) are responsible for establishing their own policies that address their physical and environmental requirements.]*	AWS has established a Physical and Environment Protection Policy that 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.
5.9.1 – Physically Secure Location	*[Customers (or their partners) are responsible for any applicable security perimeter requirements for their facilities.]*	AWS has developed formal, documented physical and environmental protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policy is reviewed on an annual basis.

5.9.1.1 – Security Perimeter	*[Customers (or their partners) are responsible for any applicable security perimeter requirements for their facilities.]*	Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Physical access points to server locations are managed by electronic access control devices, requiring proper multi-factor authorization to access them.
5.9.1.2 – Physical Access Authorizations	*[Customers (or their partners) must implement a process to control secure locations in accordance with this control.]*	Physical access to all AWS data centers, collocations, and facilities housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Authorization credentials, which include an electronic access badge (unique to the employee, vendor or contractor) and PIN—are provided to authorized personnel in order to physically access the data center facilities. On a quarterly basis, access lists and authorization credentials of personnel with access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). Personnel are removed from the list when access is no longer required.
5.9.1.3 – Physical Access Control	*N/A*	AWS utilizes multi-factor authentication mechanisms for data center access as well as additional security mechanisms to ensure that only authorized individuals enter an AWS data center. Individual access authorizations are verified electronically via the electronic access control system, which authenticates the cardholder's badge and PIN against the system's database to permit the cardholder to enter the data center.

		Physical access to the data centers within the system boundary is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. AWS data centers utilize trained security guards 24x7, who are stationed at the building entrance. Entry areas are the only publically accessible areas of data centers within the system boundary. Entry areas of the data centers are where non-permanent personnel check-in and where these personal are also validated as authorized personnel prior to accessing the data center. Physical keys to access the data center server, networking, electrical and mechanical rooms are secured by the data center manager, in a lockbox, with a sign out/sign in sheet. The AWS Security Operations Center reviews the list of card readers maintained in the AWS physical access management system against the data center blueprints for inventory accuracy. Keys are changed in accordance to fire code regulations in the local jurisdiction of the data center location or when keys are lost or compromised. Inventory of keys is accounted for on an annual basis.
5.9.1.4 – Access Control for Transmission Medium	*N/A*	Restricted areas such as server rooms and data centers are kept locked at all times, thus, requiring proper authorization to access them via the use of an authorized badge and PIN. Transmission lines within buildings, both hidden and visible, as well as the cables outside of buildings are protected from accidental damage, disruption, and physical tampering by the use of secure conduit.

5.9.1.5 – Access Control for Display Medium	*[This is a customer and/or partner responsibility. AWS systems do not display CJI information.]*	AWS implements physical and environmental protection (PE-5) access controls for output devices that have been assessed and accredited under FedRAMP. Specific to the CJIS requirement, AWS does not have any devices that would display CJI information.
5.9.1.6 – Monitoring Physical Access	*N/A*	AWS monitors physical access to the information system to detect and respond to physical security incidents via video surveillance, electronic access controls, and intrusion detection systems. Physical access logs are reviewed on a daily basis. On a daily basis, all access provisioned events as well as access events are reviewed by the infrastructure compliance team. Physical access reviews and investigations are coordinated with AWS Security Operations Center, and forced or suspicious physical access activities are reported. Real-time physical intrusion alarms and surveillance are monitored by the Alarm Monitoring application within AWS physical access management system, which alerts local data center security guards and the Security Operation Center of physical intrusions.
5.9.1.7 – Visitor Control	*N/A*	Visitor access records are captured in two forms —the onsite data center visitor sign-in sheet and data center visitor access request tickets stored in AWS's trouble ticketing system. Badge access records (physical access granted/denied badge reader events) are captured and stored within AWS's physical access management system. On a monthly basis, visitor access sign-in sheets are reviewed by the data center Area Access Manager (AAM)

		to help ensure that each visitor listed on the sign-in sheet had an associated approved trouble ticket.
5.9.1.8 – Delivery and Removal	*N/A*	All equipment entering or exiting 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	*N/A*	AWS meets all requirements defined for a "physically secure location".

5.10 – Policy Area 10: System and Communications Protection and Information Integrity	*[Customers (or their partners) should address this control within their AWS systems, as well as within their physical infrastructure.]*	All network fabrics that are part of the AWS cloud are separated by boundary protection devices that control the flow of information between these fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) residing on these devices. ACLs are defined, approved by appropriate Amazon's Information Security team, managed and deployed using a proprietary tool. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed, approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected.
5.10.1 – Information Flow Enforcement	*[Customers (or their partners) are responsible for properly implementing VPC's security groups and network ACLs.*	Network devices, including firewalls 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 protection devices employ rule sets, ACLs, and configurations to enforce the flow of information to specific information system services.

5.10.1.1 – Boundary Protection	*[Customers (or their partners) have the ability to dynamically isolate their AWS assets through the use of security groups and network ACLs in VPC.* *Customer EC2 instances may initiate outbound traffic to the internet. It is a customer responsibility to route this traffic through authenticated proxy servers. This can be implemented with an EC2 instance acting as a proxy. Traffic can also be routed through a site-to-site VPN connection between the customers VPC to the customer's network infrastructure and out to the internet through their existing TIC or internet proxy.* *A Federal government customer can configure a site-to-site VPN connection between AWS and their network infrastructure. Information being transmitted by a Federal government agency to external entities would exit the agency's network following normal traffic patterns through the TIC, which would allow data transmissions to be inspected by the TIC processes.* *Customers must setup and configure a VPC in order to virtually allocate publicly accessible information system components to separate sub-networks with separate physical network interfaces. VPC also provides customers with an IPsec VPN. An IPsec VPN connection connects a customer's VPC to another network designated by the customer. VPC customers can create an IPsec VPN connection to their VPC by first establishing an Internet Key Exchange (IKE) security association between their VPC VPN gateway and another network gateway using a pre-shared key as the authenticator.* *For more information please see:* • *https://aws.amazon.com/whitepapers/aws-security-best-practices/*	AWS provides customers with secure HTTP access (HTTPS) to their AWS storage or compute instances using API endpoints. AWS also implements dedicated network devices to manage 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 using dedicated network devices.

	- *http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html]*	
5.10.1.2 – Encryption	*[Customers (or their 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 (or their partners) can also connect remotely to their Windows instances using Remote Desktop Protocol (RDP) by utilizing an RDP certificate generated for their instance.]*	AWS ensures that the message contents are not readable in transit by using symmetric encryption of data before transmission. SSL or TLS sessions terminate at load balancers or, for Amazon S3 connections, at the web servers. Both the load balancers and the web servers employ OpenSSL. Available cryptographic ciphers include: AES-256-CBC, AES-128-CBC, and 3DES-EDE-CBC.
5.10.1.3 – Intrusion Detection Tools and Techniques	*[Customers (or their partners) are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments. In addition to monitoring tools that the customer may install within the customer's EC2 instances, they may also make use of CloudTrail and CloudWatch to provide additional monitoring capabilities for their systems hosted on AWS.]*	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: • Port scanning attacks • Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) • Application performance metrics • Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming

		mechanisms determined by AWS service and Security teams.
5.10.1.4 – Voice over Internet Protocol	*N/A*	N/A
5.10.1.5 – Cloud Computing	*N/A*	After demonstrating compliance with the FedRAMP security requirements, the AWS US regions have been authorized. AWS GovCloud (US), has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for moderate and high impact levels. The services in scope of the AWS GovCloud (US) JAB P-ATO boundary at high baseline security categorization can be found within AWS Services in Scope by Compliance Program at https://aws.amazon.com/compliance/services-in-scope/. For a complete list of authorizing agencies who have issued an ATO on AWS GovCloud (US), please visit https://www.fedramp.gov/marketplace/compliant-systems/

		AWS US East-West, has been granted multiple Agency ATOs for moderate impact level. The services in scope of the AWS US East-West authorization boundary can be found on AWS Services in Scope by Compliance Program at https://aws.amazon.com/compliance/services-in-scope/. For a complete list of authorizing agencies who have issued an ATO on AWS US East-West please visit https://www.fedramp.gov/marketplace/compliant-systems/
5.10.2 – Facsimile Transmission of CJI	*N/A*	N/A
5.10.3 – Partitioning and Virtualization	*[Customers (or their 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.]*	Amazon EC2 currently utilizes a highly customized hypervisor, taking advantage of paravirtualization (in the case of Linux guests). 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. The CPU provides four separate privilege modes: 0-3, called rings. Ring 0 is the most privileged and 3 the least. The host OS executes in Ring 0. However, rather than executing in Ring 0 as most operating systems do, the guest OS runs in a lesser-privileged Ring 1 and applications in the least privileged Ring 3. This explicit virtualization of the physical resources leads to a clear separation between guest instances and the hypervisor, resulting in additional security given the separation between the two.

5.10.3.1 – Partitioning	*[Customers (or their partners) are responsible for properly implementing security function isolation within any EC2 instances.]*	AWS is responsible for security function isolation for the AWS Infrastructure.
5.10.3.2 – Virtualization	*[Customers (or their partners) 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. Customers (or their partners) should review their options for setting up EC2 instances and machine images.]*	AWS uses 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.
5.10.4 – System and Information Integrity and Policy Control	*N/A*	N/A

5.10.4.1 – Patch Management	*[For all Change Management controls, AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration and change control of their systems deployed on AWS. Additionally, customers (or partners) are responsible for flaw identification and flaw remediation within their systems hosted on AWS. Customers are responsible for performing operating system vulnerability scanning, web application, and database scanning (as applicable) for assets for which they have implementation responsibility (above the hypervisor).]*	AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third party vendor at least annually, and all identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored, evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website.
5.10.4.2 – Malicious Code Protection	*[Customers (or their partners) are responsible for deploying, updating and managing anti-malware mechanisms at the customer's EC2 instances, in accordance with their organization's anti-malware policies and procedures.]*	The AWS infrastructure is built primarily on a customized Linux-based environment. In order to protect against malicious code, AWS uses a combination of internal research, open source community-distributed software alerts, and special support contracts that allow it 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.
5.10.4.3 – Spam and Spyware Protection	*[Customers (or their partners) are responsible for detecting and preventing spam and spyware on the AWS systems and services that they deploy.]*	Because the AWS infrastructure is not connected to e-mail servers and is heavily Linux based, it has limited exposure to spam and spyware. Malware mitigation practices are in place across the infrastructure.

5.10.4.4 – Security Alerts and Advisories	*[Customers (or their partners) are responsible for monitoring security alerts and advisories and taking appropriate action as required by this control.]*	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	*[Customers (or their partners) are responsible for restricting the information input to any connection to FBI CJIS services to authorized personnel only.]*	N/A
5.11 – Policy Area 11: Formal Audits	*[Customers (or their partners) are responsible for conducting formal audits to ensure compliance with applicable statutes, regulations and policies.]*	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 – Audits by the FBI CJIS Division	*N/A*	N/A
5.11.1.1 – Triennial Compliance Audits by the FBI CJIS Division	*[Customers (or their partners) are responsible for supporting FBI CJIS Division audits and, when applicable, requesting support from AWS.]*	AWS is committed to complying with all FBI CJIS Security Policy requirements
5.11.1.2 – Triennial Security Audits by the FBI CJIS Division	*[Customers (or their partners) are responsible for supporting FBI CJIS Division audits and, when applicable, requesting support from AWS.]*	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.

5.11.2 – Audits by the CSA	*[Customers (or their partners) are responsible for supporting FBI CJIS Division audits and, when applicable, requesting support from AWS.]*	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.
5.11.3 – Special Security Inquiries and Audits	*[Customers (or their partners) are responsible for supporting FBI CJIS Division audits and, when applicable, requesting support from AWS.]*	AWS is a FedRAMP authorized CSP and was assessed by an accredited 3PAO.
5.12 – Policy Area 12: Personnel Security	*[Customers (or their partners) are responsible for establishing their own personnel security policies.]*	AWS maintains a formal, documented personnel security policy. The policy is reviewed and updated annually, and disseminated to all employees, vendors, and contractors using an internal policy web portal.

5.12.1 – Personnel Security Policy and Procedure	*N/A*	N/A
5.12.1.1 – Minimum Screening Requirements for Individuals Requiring Access to CJI	*[Customers (or their partners) are responsible for properly screening personnel prior to granting access to their systems hosted 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 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.
5.12.1.2 – Personnel Screening for Contractors and Vendors	*[Customers (or their partners) should ensure contractors' identification is verified via the state of residency and national fingerprint-based record check.]*	AWS has established formal policies and procedures to address this control.

5.12.2 – Personnel Termination	*[Customers (or their partners) are responsible for properly terminating access for personnel to whom they have granted access.]*	AWS is responsible for the following processes upon the termination of an employee: • Communicating termination responsibilities, such as security requirements, legal responsibilities, and non-disclosure obligations to terminated personnel. • Revoking information system access. • Retrieving all AWS information system-related property (e.g. authentication tokens, keys, badges). • Disabling badge access (automated).
5.12.3 – Personnel Transfer	*[Customers (or their partners) should address this control within their AWS environment using 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	*[Customers (or their partners) should address this control within their AWS environment using 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.

5.13 – Policy Area 13: Mobile Devices	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	Wireless access points are not allowed within the system boundaries. Wireless access is not permitted within the AWS infrastructure. Additionally, mobile devices are not a part of the AWS boundary and not permitted as a part of the infrastructure.
5.13.1 – Wireless Communications Technologies	*N/A*	N/A
5.13.1.1 – All 802.11x Wireless Protocols	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	Wireless access points are not allowed within the system boundaries. Wireless access is not permitted within the AWS infrastructure.

5.13.1.2 – Cellular	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	Cellular devices are not allowed within the system boundary. Cellular devices are not permitted to connect to the AWS infrastructure.
5.13.1.2.1 – Cellular Service Abroad	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	Cellular devices are not allowed within the system boundary. Cellular devices are not permitted to connect to the AWS infrastructure.
5.13.1.2.2 – Voice Transmissions Over Cellular Devices	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A

5.13.1.3 – Bluetooth	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.1.4 – Mobile Hotspots	*N/A*	N/A
5.13.2 – Mobile Device Management (MDM)	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A

5.13.3 – Wireless Device Risk Mitigations	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.4 – System Integrity	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.4.1 – Patching/Updates	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A

5.13.4.2 – Malicious Code Protection	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.4.3 – Personal Firewall	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.5 – Incident Response	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A

5.13.6 – Access Control	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.7 – Identification and Authentication	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.7.1 – Local Device Authentication	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A

5.13.7.2 – Advanced Authentication	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.7.2.1 – Compensating Controls	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A
5.13.7.3 – Device Certificates	*[Customers (or their partners) should address this control within their AWS environment using appropriate policies and procedures.]*	N/A

Document Revisions

Date	Description
March 2017	Updates to Criminal Justice Information Service Security Policy 5.5.
November 2016	Initial document