This paper has been archived.

For the latest compliance content, see https://aws.amazon.com/compliance/resources/.

Criminal Justice Information Service Compliance on AWS

(This document is part of the CJIS Workbook package, which also includes CJIS Security Policy Requirements, CJIS Security Policy Template, and CJIS Security Policy Workbook.)

March 2017

Archived

© 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

Archived

Contents

Archived

Abstract

There is a long and successful track record of AWS customers using the AWS cloud for a wide range of sensitive federal and state government workloads, including Criminal Justice Information (CJI) data. Law enforcement customers (and partners who manage CJI) are taking advantage of AWS services to dramatically improve the security and protection of CJI data, using the advanced security services and features of AWS such as activity logging (AWS CloudTrail), encryption of data in motion and at rest (Amazon S3's Server-Side Encryption with the option to bring your own key), comprehensive key management and protection (AWS Key Management Service and AWS CloudHSM), along with integrated permission management (IAM federated identity management, multi-factor authentication).

To enable this, AWS complies with Criminal Justice Information Services Division (CJIS) Security Policy requirements where applicable, such as providing states with fingerprint cards for GovCloud administrators and signing CJIS security addendum agreements with our customers.

Archived

Introduction

Amazon Web Services (AWS) delivers a scalable cloud computing platform with high availability and dependability, providing the tools that enable customers to run a wide range of applications. Because AWS designed their cloud implementation with security in mind, you can use AWS services to satisfy a wide range of regulatory requirements, including the Criminal Justice Information Services (CJIS) Security Policy. The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to FBI CJIS systems and information for the protection and safeguarding of CJI. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination, whether at rest or in transit. This minimum standard of security requirements ensures continuity of information protection.

What is Criminal Justice Information?

Criminal Justice Information (CJI) refers to the FBI CJIS-provided data necessary for law enforcement agencies to perform their mission and enforce the laws, such as biometric, identity history, person, organization, property, and case/incident history data. CJI also refers to data necessary for civil agencies to perform their mission, including data used to make hiring decisions. CJIS Security Policy 5.2, A-3 defines CJI as:

> Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.
>
> — CJIS Security Policy 5.2, A-3

Law enforcement must be able to access CJI wherever and whenever is necessary in a timely and secure manner in order to reduce and stop crime.

Archived

What is the CJIS Security Policy

The intent of the CJIS Security Policy is to ensure the protection of the CJI until the information is 1) released to the public via authorized dissemination (e.g., within a court system, presented in crime reports data, or released in the interest of public safety) and 2) purged or destroyed in accordance with applicable record retention rules.

The Criminal Justice Information Services Division (CJIS) is a division of the United States Federal Bureau of Investigation (FBI) and is responsible for publishing the Criminal Justice Information Services (CJIS) Security Policy, which is currently on version 5.5.

The CJIS Security Policy outlines a minimum set of security requirements that create security controls for managing and maintaining Criminal Justice Information (CJI) data. The CJIS Advisory Policy Board (APB) manages the policy with national oversight from the CJIS division of the FBI. There is no centralized adjudication body for determining what is or isn't compliant with the Security Policy in the way that FedRAMP has standardized security assessments across the federal government. That means vendors/CSPs wanting to provide CJIS compliant solutions to multiple law enforcement agencies must gain formal CJIS authorizations from city, county or state level authority.

CJIS Security Addendums (Agreements)

Unlike many of the compliance frameworks that AWS supports, there is ***no*** central CJIS authorization body, no accredited pool of independent assessors, nor a standardized assessment approach to determining whether a particular solution is considered "CJIS compliant." Simply put, a standardized "CJIS compliant" solution, which works across all law enforcement agencies, does not exist. It is often falsely misunderstood and miscommunicated that a cloud service provider can be "CJIS certified". It is imperative to understand that delivering a CJIS compliant solution relies on a Shared Responsibility Model between the cloud service provider and the CJA.

Each law enforcement organization granting CJIS authorizations interprets solutions according to their own risk acceptance standard of what can be construed as compliant within the CJIS requirements. Authorizations from one state do not necessarily find reciprocity within another state (or even necessarily

Archived

within the same state). Providers must submit solutions for review with each agency authorizing official(s), possibly to include duplicate fingerprint, and background checks and other state/jurisdiction-specific requirements.

Each authorization is an agreement with that particular organization; something that must be repeated locally at each law enforcement agency. Thus, be wary of vendors that may represent themselves as having a nationally recognized or 50- state compliant CJIS service.

AWS Approach on CJIS

AWS has evaluated the 13 Policy Areas along with the 131 security requirements and has determined that 10 controls can be directly inherited from AWS, both AWS and the CJIS customer share 78, and 43 are customer specific controls. AWS has documented these requirements with a detailed workbook, which can be downloaded at CJIS Security Policy Workbook.

The AWS CJIS Security Policy Workbook outlines the shared responsibility between AWS and the CJIS customer on how AWS directly supports the requirements within our FedRAMP accreditation (Note: the CJIS Advisory Policy Board (APB) also has mapping for CJIS to NIST 800-53rev4 requirements, which are the base controls for Federal Risk and Authorization Management Program (FedRAMP) dated 6/1/2016). This document and our approach has been reviewed by the CJIS APB subcommittee chairmen, partners in the CJIS space, with favorable support on the efficacy of our workbook and approach.

CJIS and relationship to FedRAMP

All Federal Agencies, including Criminal Justice Agencies (CJA's), may leverage the AWS package completed as part of the Federal Risk and Management Program (FedRAMP). FedRAMP is a government- wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud service providers (CSP's). This approach utilizes 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 cloud adoption. FedRAMP conforms to the National Institute of Science & Technology (NIST) 800 Series Publications to verify that

Archived

all authorizations are compliant with the Federal Information Security Management Act (FISMA).

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

AWS Shared Responsibility Model

AWS offers a variety of different infrastructure and platform services. For the purpose of understanding security and shared responsibility of these AWS services, consider the following three main categories:

- Infrastructure
- Platform
- Software

Each category comes with a slightly different security ownership model based on how you interact and access the functionality. The main focus of this document, the CJIS Security Policy Template document, the CJIS Security Policy Requirements document, and the CJIS Security Policy Workbook is on the Infrastructure services. The other categories are highlighted for awareness and can also be addressed by AWS services as outlined in the following sections.

Service Categories

Infrastructure Services

This category includes compute services, such as Amazon EC2, and related services, such as Amazon Elastic Block Store (Amazon EBS), AWS Auto Scaling, and Amazon Virtual Private Cloud (Amazon VPC). With these services, you can architect and build a cloud infrastructure using technologies similar to and largely compatible with on - premises solutions. You control the operating

Archived

system, and you configure and operate any identity management system that provides access to the user layer of the virtualization stack.

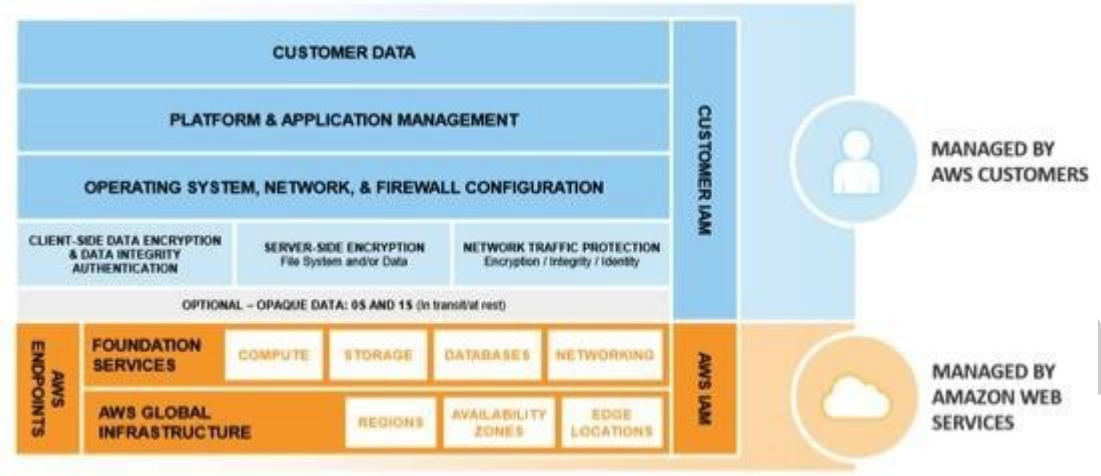


Figure 1: Shared Responsibility Model for Infrastructure Services

Platform as a Service

Services in this category typically run on separate Amazon EC2 or other infrastructure instances, but sometimes you don't manage the operating system or the platform layer. AWS provides service for these application "containers." You are responsible for setting up and managing network controls, such as firewall rules and the underlying platform – e.g., level identity and access management separately from Identity and Access Management (IAM). Examples of container services include Amazon Relational Database Services

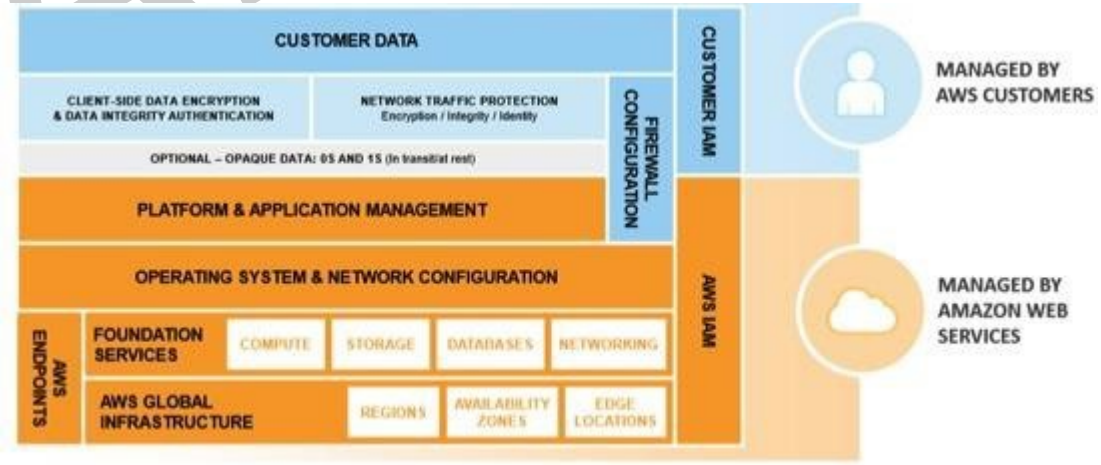


Figure 2: Shared Responsibility Model for Container Services

Archived

(Amazon RDS), Amazon Elastic Map Reduce (Amazon EMR) and AWS Elastic Beanstalk.

Software as a Service

This category includes high-level storage, database, and messaging services, such as Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon DynamoDB, Amazon Simple Queuing Service (Amazon SQS), and Amazon Simple Email Service (Amazon SES). These services abstract the platform or management layer on which you can build and operate cloud applications. You access the endpoints of these abstracted services using AWS APIs, and AWS manages the underlying service components or the operating system on which they reside. You share the underlying infrastructure, and abstracted services provide a multi-tenant platform, which isolates your data in a secure fashion and provides for powerful integration with IAM.

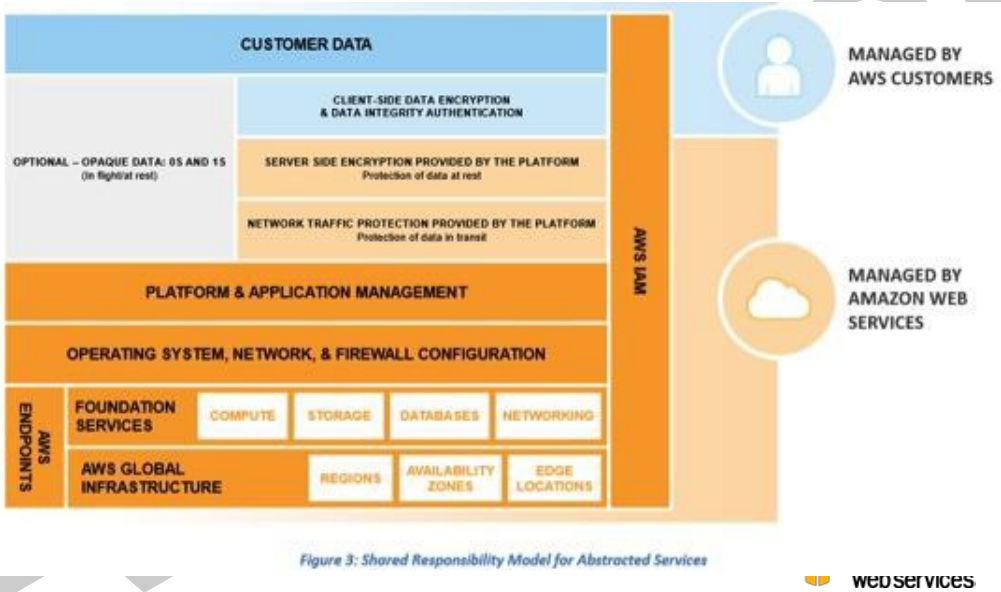


Figure 3: Shared Responsibility Model for Abstracted Services

AWS Regions, Availability Zones, and Endpoints

AWS has datacenters in multiple locations around the world. The recommended region for CJIS workloads is the AWS GovCloud region.

Regions are designed with availability in mind and consist of at least two, often more, Availability Zones. Availability Zones are designed for fault isolation. They are connected to multiple Internet Service Providers (ISPs) and different power grids. They are interconnected using high-speed links, so applications

can rely on Local Area Network (LAN0) connectivity for communication between Availability Zones within the same region. You are responsible for carefully selecting the Availability Zone(s) where your systems will reside. Systems can span multiple Availability Zones, and we recommend that you design your systems to survive temporary or prolonged failure of an Availability Zone in the case of a disaster.

AWS provides web access to services through the AWS Management Console. AWS provides programmatic access to services through Application Programming Interfaces (APLs) and command line interfaces (CLIs). Service endpoints, which are managed by AWS, provide management ("backplane") access.

Security & Compliance OF the Cloud

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

> 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."
>
> — 2.3 Risk Versus Realism

In order to manage risk and security within the cloud, a variety of processes and guidelines have been created to differentiate between the security of a cloud service provider and the responsibilities of a customer consuming the cloud services. One of the primary concepts that have emerged is the increased understanding and documentation of shared, inherited or dual (AWS & Customer) security controls in a cloud environment. A common question for

AWS is: "how does leveraging AWS make my security and compliance activities easier?" This question can be answered by demonstrating the security controls that are met by approaching the AWS Cloud in two distinct ways: first, reviewing compliance of the AWS Infrastructure gives an idea of "Security & Compliance OF the cloud"; and second, reviewing the security of workloads running on top of the AWS infrastructure gives an idea of "Security & Compliance IN the cloud".

AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. Customers running workloads on the AWS infrastructure depend on AWS for a number of security controls. AWS has several additional whitepapers, which provide additional information to assist AWS customers with integrating AWS into their existing security frameworks and to help design and execute security assessments of an organization's use of AWS. For more information, see the AWS Compliance Whitepapers.

Security & Compliance IN the Cloud

Security & Compliance **IN** the Cloud refers to how the customer manages the security of their workloads through the use of various applications and architecture (virtual private clouds, security groups, operating systems, databases, authentication, etc.)

- **Cross-service security controls** – are security controls, which a customer needs to implement across all services within their AWS customer instance.

  While each customer's use of AWS services may vary along with their own risk posture and security control interpretation, cross service controls will need to be documented within the customer's use of AWS services.

  Example: Multi-factor authentication can be used to help secure Identity and Access Management (IAM) users, groups and roles within the customer environment in-order to meet CJIS Access Management, Authentication, and Authorization requirements for the particular agency or CJIS organization.

- **Service-Specific security controls** – are service specific security implementation such as the Amazon S3 security access permission

Archived

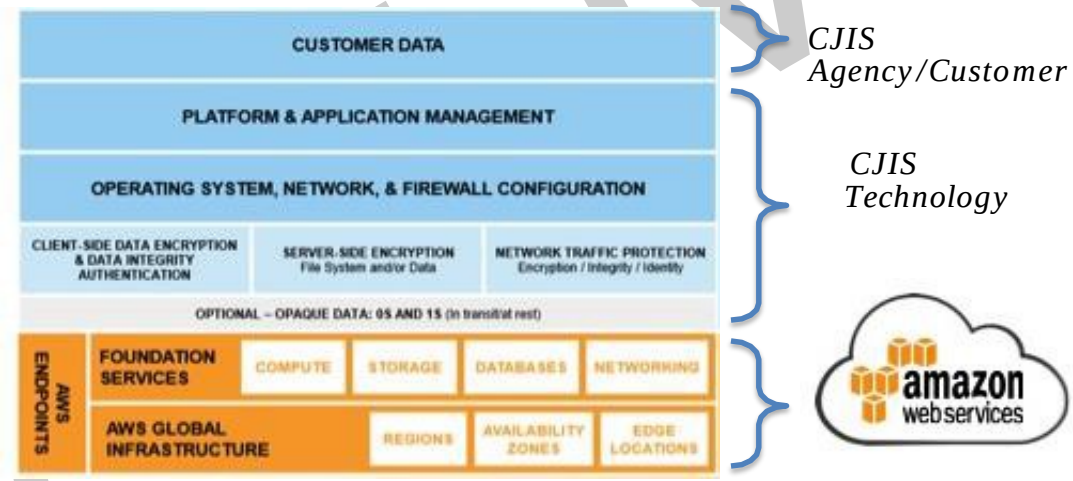
settings, logging, event notification and/or encryption. A customer may need to document service specific controls within their use of Amazon S3 in order to meet a specific security control objective related to criminal justice data and/or investigative- related records.

Example: Server Side Encryption (SSE) can be enabled for all objects classified as CJI and/or directory information related to the CJIS security.

- **Optimized Network, Operating Systems (OS) and Application Controls** – controls a customer may need to document in-order to meet specific control elements related to the use of an Operating System and/or application deployed within AWS.

  Example: Customer Server Secure hardening rules or an optimized private Amazon Machine Images (AMI) in order to meet specific security controls within Change Management.

Creating a CJIS Environment on AWS



AWS has several partner solutions that collect, transfer, 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.

Similar to other AWS compliance frameworks, the CJIS Security Policy takes advantage of the shared responsibility model between you and AWS. 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 the applicable CJIS requirements outlined in the CJIS Security Policy.

One advantage of using AWS for CJIS workloads is that you inherit a significant portion of the security control implementation from AWS and the partner solution that address and meet CJIS security policy elements.

You and your AWS customers and partners should enable several applicable security features, functions and utilize leading practices in-order to create an AWS CJIS compliant environment within their use of AWS. As such, the following section provides a high-level overview of services and tools you and your partners should consider as part of your AWS CJIS implementation.

Auditing and Accountability

(Ref. CJIS Policy Area 4)

- **AWS CloudTrail** – A 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. For more information, go here.
- **Amazon CloudWatch** – A service that monitors AWS cloud resources and the applications that you run on AWS. You can use AWS CloudWatch 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. For more information, go here.
- **AWS Trusted Advisor** – This online resource 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. For more information, go here.

Archived

- **Amazon SNS** – You can use this service 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. For more information, go here.

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.
- **AWS Identity and Access Management (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). For more information, go here.
- **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). For more information, go here.
- **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. For more information, go here.

Archived

Configuration Management

(Ref. CJIS Policy Area 7)

- **Amazon EC2** – 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). For more information, go here.
- **Amazon Machine Image (AMI)** – An 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. For more information, go here.
- **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. For more information, go here.
- **Choosing an AMI** – While AWS does provide images that can be used for deployment of host operating systems, you need to develop and implement system configuration and hardening standards to align with all applicable CJIS requirements for your operating systems. For more information, go here.
- **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. For more information, go here.
- **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, it is important to restrict access to resources based on tagging. Regardless of account structure,

Archived

you can use tag-based IAM policies to place extra security restrictions on critical resources. For more information, go here.

- **AWS Config** – 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. For more information, go here.
- **CloudFormation Templates** – Creating preapproved AWS CloudFormation templates for common use cases. Using templates allows CJIworkload 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. For more information, go here.
- **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). For more information, go here.

Media Protection & Information Integrity

(Ref. CJIS Policy Area 8 & 10)

- **AWS Storage Gateway** – A service that connects an on-premises software appliance to cloud-based storage, providing seamless and secure integration between your on-premises IT environment and AWS's storage infrastructure. For more information, go here.
- **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 you to make data easily accessible to your applications or for backup purposes. Before you store sensitive data, you should use CJIS requirements for restricting direct inbound and outbound data to select the correct storage option.

Archived

For example, Amazon S3 can be configured to encrypt your data at rest with server-side encryption (SSE). In this scenario, 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, you can use one of the following methods:

- **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. AWS KMS 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, AWS KMS provides a convenient management option for creating and administering the keys used to encrypt your data at rest. For more information, go here.
- **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. For more information, go here.
- **AWS CloudHSM Service** – A service that 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. For more information, go here.

System and Communication Protection and Information Integrity

(Ref. CJIS Policy Area 10)

- **AWS Virtual Private Cloud (VPC)** – You can use VPC to connect existing infrastructure to a set of logically isolated AWS compute

Archived

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. For more information, go here.

- **AWS Direct Connect (DX)** – AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. For more information, go here
- **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. SSL/TLS clients can use these cipher suites 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** – You should implement SSL encryption on your server instances. You 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.

AWS security engineers and solution architects have developed whitepapers and operational checklists to help you select the best options for your needs and recommend security best practices. For example, guidance on securely storing and rotating or changing secret keys and passwords.

Archived

Conclusion

There are few key points to remember in supporting CJIS workloads:

Security is a shared responsibility - as AWS doesn't manage the customer environment or data, this means you are responsible for implementing the applicable CJIS Security Policy requirements in your AWS environment, over and above the AWS implementation of security requirements within the infrastructure.

Encryption of data in transit and at rest is critical - AWS provides several "key" resources to help you achieve this important solution. From Solutions Architect personnel available to assist you to our Encrypting Data at Rest Whitepaper, as

well as multiple Encryption leading practices, AWS strives to provide the resources you need to implement secure solutions.

AWS directly addresses the relevant CJIS Security Policy requirements applicable to the AWS infrastructure. As AWS provides a self-provisioned platform that customers wholly manage, AWS isn't directly subject to the CJIS Security Policy. However, we are absolutely committed to maintaining world-class cloud security and compliance programs in support of our customer needs. AWS demonstrates compliance with applicable CJIS requirements as supported by our third-party assessed frameworks (such as FedRAMP) incorporating on-site data center audits by our FedRAMP accredited 3PAO.

In the spirit of a shared responsibility philosophy, the AWS CJIS Requirements Matrix and the CJIS Security Policy Workbook (in a system security plan template) have been developed, which aligns to the CJIS Policy Areas. The Workbook is intended to support customers in systematically documenting their implementation of CJIS requirements alongside the AWS approach to each requirement (along with guidance on submitting the document for review and authorization).

AWS provides multiple built-in security features in support of CJIS workloads such as:

- Secure access using AWS Identity and Access Management (IAM) with multi-factor authentication
- Encrypted data storage with either AWS provided options or customer maintained options
- Logging and monitoring with Amazon S3 logging, AWS CloudTrail, Amazon CloudWatch, and AWS Trusted Advisor
- Centralized, customer controlled key management with AWS CloudHSM and AWS Key Management Service (KMS)

Further Reading

For additional help, see the following sources:

- AWS Compliance Center: http://aws.amazon.com/compliance

Archived

- 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: https://d0.awsstatic.com/whitepapers/compliance/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: https://aws.amazon.com/compliance/public-sector-contact/

Document Revisions

Date	Description
March 2017	Revised for 5.5, combined CJIS 5.4 Workbook and CJIS Whitepaper.
July 2015	First publication.

Archived