Building CJIS Compliant Solutions in AWS GovCloud (US)

October 2019

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. 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.

What is the CJIS Security Policy?

The Criminal Justice Information Services (CJIS) Security Policy provides a set of security requirements to protect and safeguard FBI-provided Criminal Justice Information (CJI) used by law enforcement and civil agencies to accomplish their missions. CJI includes biometric, identity history, biographic, property, and case/incident history data. Sections 1.1 and 1.2 outline the purpose and scope of the CJIS Security Policy as providing "appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit" and "guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI."

The CJIS Security Policy outlines security controls covering training, personnel security, technical security, and physical security. Of the thirteen (13) CJIS Security Policy Areas, four of the most fundamental policy areas applicable to a customer's cloud architecture include:

- Policy Area 2 Security Awareness Training
- Policy Area 9 Physical Security
- Policy Area 10 System and Communications Protection and Information Integrity
- Policy Area 12 Personnel Security

These four sections of the CJIS Security Policy present two distinct approaches to protecting CJI:

1) Secure CJI utilizing strong, federally validated encryption to protect sensitive information in-transit and at-rest regardless of its physical location, and limit access to CJI to only those with logical access to both the encrypted data and encryption keys.
2) Rely on physical security, background checks, and training to protect CJI stored or transmitted in clear text format within a physical location.

Encryption: The "Key" to CJIS compliance in the Cloud

The CJIS Security Policy requires that "[w]hen CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption."[1] The policy also goes on to require that "[w]hen CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption."[2] To fully understand when the policy requires data to be encrypted, it is important to understand what is meant by being "outside the boundary" of a "physically secure location" and how this impacts the implementation of personnel security controls contained in CJIS Security Policy Areas 2 (Security Awareness Training) and 12 (Personnel Security), which both leverage the definition of "physically secure location" when defining obligations for personnel training and screening. Both policy areas require that the controls in the respective sections "apply to all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas."[3] Personnel meeting this definition are subject to the personnel security and training requirements, which mandate federal and state-of-residence fingerprint background checks and security awareness training. These requirements also apply to personnel with access to encryption keys used to secure CJI.

The CJIS Security Policy defines a "physically secure location" as "a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems."[4] The establishment of a "physically secure location" as defined under the CJIS Security Policy has been the traditional method employed to secure facilities owned or controlled by criminal justice or non-criminal justice agencies where there is a technical or operational need to view, handle, store or transmit CJI in an unencrypted or human accessible

[1] Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, page 54, Section 5.10.1.2.1
[2] Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, page 55, Section 5.10.1.2.2
[3] Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, page 63 Section 5.12 paragraph 1
[4] Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, page 51 Section 5.9.1

state. In lieu of logical security controls designed to protect data from unauthorized access, such locations require that adequate personnel, physical, and technical controls be implemented to protect unencrypted and human accessible CJI from unauthorized access and viewing.

Agencies using solutions built on AWS are empowered to leverage resilient and secure information systems protected by a strong virtual boundary, combined with customer-managed access controls and monitoring capabilities regardless of its physical location. Encrypting CJI in transit and at rest using symmetric encryption keys managed by a law enforcement agency or trusted partners, and processing CJI within the customer controlled Virtual Private Cloud (VPC), means that customers can eliminate AWS employees from being within the scope for CJIS background checks or security awareness training requirements. This approach is consistent with the principle of least privilege and allows AWS customers to retain complete control of their own data. As it pertains to demonstrating CJIS compliance with physical and personnel security requirements, the combination of strict access controls and logical separation of the AWS Virtual Private Cloud with strong encryption where customers manage their own keys eliminates the need to enforce, audit and validate the physically secure location and personnel security requirements for cloud data centers. AWS customers continue to inherit the secure design of AWS GovCloud (US) facilities but are not reliant on physical and personnel security as a primary means of security and compliance.

To help customers meet the CJIS Security Policy requirements for storing, transmitting and processing CJI outside of the boundary of a physically secure location AWS provides a collection of powerful customer managed access control and data protection services. These services include FIPS 140-2 validated end-points for protection of CJI in-transit and FIPS-197 encryption for protection of CJI at-rest. A critical element of secure encryption is the management of the encryption keys. AWS GovCloud (US) offers a Key Management Service (KMS) that uses FIPS 140-2 validated hardware security modules, allowing customers to create, own, and manage their own symmetric master keys. These customer master keys never leave the AWS KMS FIPS validated hardware security modules unencrypted and are not visible to AWS personnel. These encryption tools in the AWS GovCloud (US) regions help AWS customers comply with CJIS data protection requirements and align to the best security practices found in Appendix G-3 of the CJIS Security Policy: "Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI..."[5] By following these CJIS best practices, AWS criminal justice customers can be confident that their CJI stored, transmitted and processed on AWS is consistently protected while at rest, in transit, or in-process, not just within the confines of the police station, jail, courthouse or datacenter.

Criminal Justice professionals face daily challenges that take them out into the communities they serve. These professionals deserve systems that can provide consistent, reliable, resilient, secure and compliant information systems wherever the job may take them. AWS provides tools to help build these systems; and allows for secure access to CJI anytime and anywhere.

[5] Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, page G-18 number 1