VMware Cloud on AWS GovCloud Criminal Justice Information Services (CJIS) Whitepaper

vmware

Table of contents

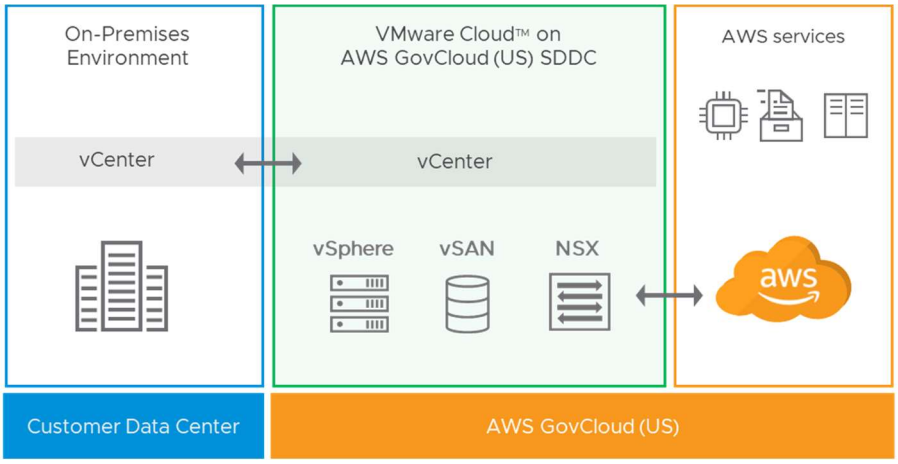
CJIS SECURITY POLICY AREAS

1. Information Exchange Agreements
2. Security Awareness Training
3. Incident Response
4. Auditing and Accountability
5. Access Control
6. Identification and Authentication
7. Configuration Management
8. Media Protection
9. Physical Protection
10. System and Communications Protection and Information Integrity
11. Formal Audits
12. Personnel Security
13. Mobile Devices

VMware Cloud on AWS GovCloud

The VMware Cloud (VMC) on AWS GovCloud is an Infrastructure as a Service (IaaS) government community cloud intended for sole use of U.S. federal, tribal, state, and local government customers, U.S. higher education, U.S. government contractors, and Federally Funded Research and Development Center (FFRDC) organizations that have requirements for a high-impact system security categorization cloud.

The VMC on AWS GovCloud service integrates VMware's compute, storage, and network virtualization products (vSphere, vSAN, and NSX, respectively) and optimizes them to run on dedicated, elastic, bare-metal AWS GovCloud infrastructure. The integration of these products is referred to as a Software Defined Data Center (SDDC).



VMC enables customers with self-service cloud infrastructure that deploys VMware's SDDC for customer use. This capability allows a customer to run the same software stack in the cloud as in their on-premises datacenter.

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 Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI).

The FBI does not provide a formal CJIS certification, each agency is individually responsible for assessing and ensuring that their information systems meet the CJIS requirements. The FBI operates a shared management philosophy that with federal, state, local, and tribal law enforcement agencies. Where agencies engage with vendors to process CJIS data, they must enter into a contract related to administration of criminal justice information with the vendor before they begin to work with the vendor

Relationship between CJIS and FedRAMP

The CJIS Security policy derives its guidance not only from the FBI directives but also leverages a number of technical requirements from the guidance from the National Institute of Standards and Technology (NIST). The Federal Risk and Authorization Management Program or FedRAMP provides a standard approach to assessing and authorizing cloud service providers. The NIST's Special Publication

[SP] 800-53 serves as a key security and compliance baseline for the Federal Risk Authorization Management Program (FedRAMP). VMware Cloud on AWS GovCloud has implemented security controls in line with the FedRamp High requirements, meaning several requirements in the CJIS security policy are met through the implementation of controls prescribed in the FedRAMP. The VMware Cloud on AWS GovCloud service is currently under 'Agency Review' for FedRAMP High authorization.

How VMware Cloud on AWS GovCloud addresses CJIS Security Policy requirements

The CJIS Security Policy specifies 13 policy areas for protecting criminal justice information, as well as maintaining data privacy and information security. The policy requires agencies and vendors to implement measures to protect CJI data during storage, transmission, viewing, modification, or destroying the CJI data.

VMware Cloud on AWS GovCloud has produced a detailed CJIS mapping workbook that describes how we address each requirement within these 13 policy areas in the CJIS security policy. Agencies can leverage this workbook to evaluate VMware Cloud on AWS GovCloud service against their requirements and understand the shared responsibilities between VMware, Agency and FBI when planning, implementing and migrating the workloads to VMware Cloud on AWS GovCloud.

As indicated above, VMware Cloud on AWS GovCloud has implemented controls in line with the FedRAMP requirements. This allows us to address several requirements in the CJIS Security Policy.

One of the key requirements in the CJIS security policy is encryption of data outside the boundary of the physical secure location. VMware Cloud on AWS GovCloud uses FIPS-validated cryptographic protections to protect administrative and customer data in-transit internal to the system and leaving the authorization boundary. All encryption for AWS services in VMC on AWS GovCloud is backed by FIPS 140-2 validated AWS Key Management Service (KMS).

For data at rest, VMware Cloud on AWS GovCloud leverages the vSAN encryption. vSAN uses AWS Key Management Service (KMS) to generate the Customer Master Key (CMK). The AWS KMS service uses FIPS 140-2 validated hardware security modules (HSMs) to protect the confidentiality and integrity of all customer keys. This use of encryption in transit and rest, combined with use of AWS KMS and processing CJI within the customer managed SDDC eliminates any VMware personnel from having access to CJI data, meaning VMware personnel can be eliminated from being within scope for CJIS background checks and security awareness training requirement.

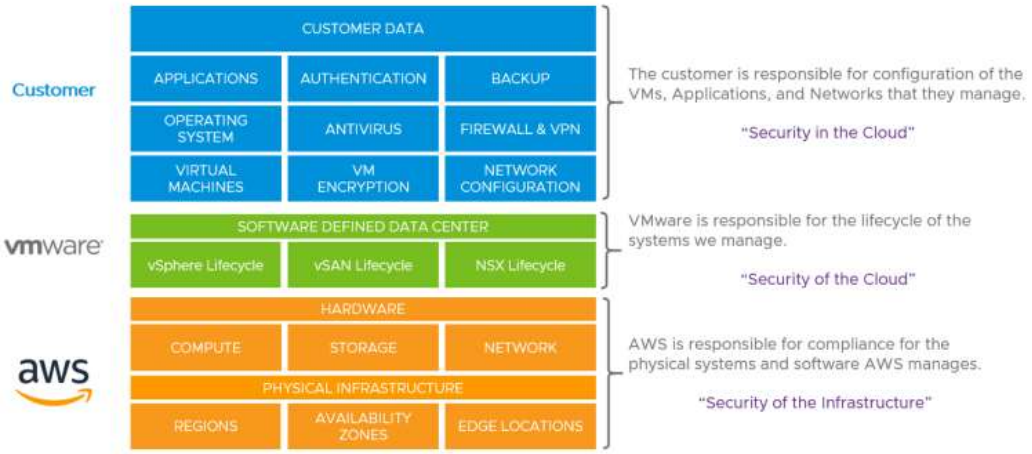
VMware Cloud on AWS GovCloud also signs the CJIS Security Addendum to confirm that our IT systems and practices are consistent with the CJIS Security Policy.

For further details on how VMware Cloud on AWS GovCloud addresses CJIS security policy requirement, we recommend you see our VMware Cloud on AWS CJIS Mapping Workbook.

Deploying an SDDC in the VMware Cloud on AWS GovCloud environment

Before deploying the workloads to VMware Cloud on AWS GovCloud, we recommend agencies evaluate the VMware CJIS – Mapping Workbook and make their own independent assessment of our solution. VMware Cloud on AWS

GovCloud operates on a shared responsibility model, with customers owning for maintaining security of the workloads they deploy on our platform, VMware managing the security of the IaaS platform and AWS responsible for the security of the physical infrastructure. For further details on Shared Responsibility Model see *vmware-shared-responsibility-model-overview-vmware-cloud-on-aws.pdf*



For technical considerations around deploying an SDDC on the VMware Cloud on AWS GovCloud see *VMware Cloud on AWS GovCloud Getting Started Guide*

Conclusion

Cloud computing technology allows the Federal Government to address demand from for better, faster services and to save resources, consolidate services, and improve security. Our compliance offerings are continually evolving, we are currently under 'Agency Review' for FedRAMP and DOD CC SRG. VMware is committed to supporting government agencies address critical security and compliance mandates, including the CJIS security policy requirements and provide an intrinsically secure and robust cloud service that U.S. Government agencies can rely upon for their cloud needs.

Additional reading

- *CJIS Security Policy Resource Center — FBI*
- *CJIS Cloud Control Catalog — FBI*
- *VMware Cloud on AWS GovCloud (US)*
- *Trust Center (vmware.com)*


vmware