WHITE PAPER–SEPTEMBER 2022

Compliance with International Traffic in Arms Regulations (ITAR)

VMware Cloud on AWS GovCloud (US)

Table of contents

Introduction to ITAR

The International Traffic in Arms Regulation (ITAR) is a United States export control regulation that regulates the export of defense and military technologies. The *United States Munitions List* (USML) defines 21 categories of items subject to these export controls; organizations are subject to ITAR if their data falls into one of these categories.

ITAR mandates that information can only be shared with US Persons unless under special authorization or exemption. US Persons are individuals who are US Citizens or Green Card (Permanent Resident Card) holders.

There is no formal certification or accreditation process for ITAR. However, the VMware Cloud on AWS GovCloud (US) service supports customers with ITAR-controlled data.

How VMware Cloud on AWS GovCloud (US) supports ITAR compliance

The VMware Cloud (VMC) on AWS GovCloud is an Infrastructure as a Service (IaaS) government community cloud intended for sole use by 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.

Jointly engineered by VMware and AWS, this on-demand, scalable service enables IT teams to seamlessly extend, migrate, protect, and manage their cloud-based resources with familiar VMware tools. With the same architecture and operational experience on-premises and in the cloud, US public sector IT teams can now quickly derive instant value through the AWS and VMware hybrid cloud experience while meeting the most stringent security and compliance requirements including ITAR.

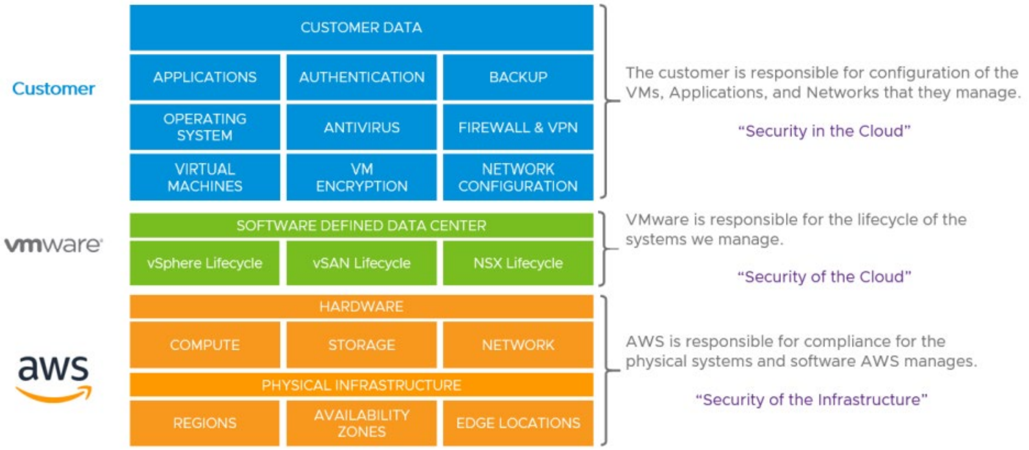
VMC on AWS GovCloud (US) is deployed in the AWS GovCloud (US-West) and (US-East) regions, physically located in the United States. The service is operated by VMware employees who are US citizens on US soil. The service is continuously audited by an independent third-party assessment organization (3PAO) accredited by the Federal Risk Authorization Management Program (FedRAMP) and has been authorized for use at the High impact level by the FedRAMP Joint Authorization Board (JAB). FedRAMP High authorization recognizes that VMware Cloud on AWS GovCloud (US) can run highly sensitive government workloads with the hardened security and production-grade capabilities that government agencies require. This authorization continues our commitment to support security and compliance requirements of agencies maintaining ITAR data in the VMware Cloud on AWS GovCloud (US) region. You can view the FedRAMP Authorization status of the service in the *FedRAMP Marketplace*.

VMware does not have any visibility into the data that customers have uploaded into the service, so all customer data within VMC on AWS GovCloud (US) is treated as ITAR data. Customers who have ITAR regulated data can successfully and run workloads on VMC on AWS GovCloud (US) platform. For more details on the service, see *VMware Cloud on AWS GovCloud (US).*

Customers who require additional disaster recovery capabilities can also opt for the VMware Site Recovery (VSR) service. The service provides an end-to-end disaster recovery solution that can help reduce the requirements for a secondary recovery site, accelerate time-to-protection, and simplify disaster recovery operations. The VSR service is available as an optional add-on service for VMC on AWS GovCloud (US). For details on VSR please visit *VMware Site Recovery | Disaster Recovery as a Service.*

VMware Cloud on AWS GovCloud (US) Shared Responsibility Model

VMware Cloud on AWS GovCloud (US) implements a shared responsibility model that defines distinct roles and responsibilities of the three parties involved in the offering: Customer, VMware, and Amazon Web Services.



Customer responsibility "Security in the Cloud" – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS GovCloud (US) User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

VMware responsibility "Security of the Cloud" – VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS GovCloud (US) service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS GovCloud (US).

AWS responsibility "Security of the Infrastructure" – AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service.

When migrating ITAR data, customers should be aware of their responsibilities to manage ITAR data including access governance, data classification, roles and permissions, virtual machine patching and monitoring and responding to security incidents over their environment and maintaining any necessary addendums/contractual documentation to meet ITAR compliance. Customers should also conduct their own risk assessments to identify any applicable compliance requirements for the data they upload on to the VMC platform and any contractual commitments to be included in the addendum/terms of service. For further details reach out to VMware sales representative or see *VMware Cloud on AWS GovCloud Service Description*.

Conclusion

VMware Cloud on AWS GovCloud (US) has been built with stringent security measures keeping in mind the security, availability, and confidentiality requirements of US public sector agencies across various departments. Our compliance with the FedRAMP High baseline requirements demonstrates the robust controls and measures in place to protect ITAR data and host the relevant workloads onto our platform.

VMware regularly conducts various internal and external security assessments and audits to protect our platform and maintain customers' trust in securing their data. VMware is committed to working with agencies on their ITAR requirements. Where agencies wish to understand specific areas in more depth, VMware can assist agencies by providing further resources in line with a specific use case.

Further reading

- VMware Cloud on AWS GovCloud listing in the FedRAMP Marketplace
- VMware Cloud on AWS GovCloud Service Description
- VMware Cloud on AWS GovCloud (US)
- VMware Site Recovery

Contributors

- Moin Nawaz Syed – Product Line Manager, VMware Cloud Solutions
- Patrick O'Brien – Group Product Line Manager, VMware Cloud Solutions
- Matt Dreyer – Sr. Director, VMware Cloud Solutions

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.