Compliance with Internal Revenue Service (IRS) Publication 1075
VMware Cloud on AWS GovCloud
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>VMware Cloud on AWS GovCloud (US)</td>
<td>3</td>
</tr>
<tr>
<td>Mandatory requirements for an FTI in a cloud computing environment</td>
<td>4</td>
</tr>
<tr>
<td>Conclusion</td>
<td>8</td>
</tr>
<tr>
<td>Further reading</td>
<td>8</td>
</tr>
<tr>
<td>Contributors</td>
<td>8</td>
</tr>
</tbody>
</table>
**Introduction**

The United States Internal Revenue Service’s (IRS) goal is to promote taxpayer confidence in the integrity of the tax system by ensuring confidentiality of the tax information provided to the federal, state and local agencies. The IRS 1075 publication provides guidance to agencies, agents, contractors and subcontractors on implementing adequate policies, processes, controls and safeguards to protect Federal tax information (FTI).

The IRS 1075 requirements follow the FedRAMP and NIST 800-53 Rev.5 guidelines. Agencies that receive FTI must ensure that they have adequate programs in place to protect the data received in line with IRS 1075 guidelines. VMware Cloud on AWS GovCloud (US) has been authorized against the FedRAMP High baseline controls and therefore can support agencies in meeting the IRS 1075 requirements. Agencies can access VMware’s FedRAMP package at [https://marketplace.fedramp.gov/](https://marketplace.fedramp.gov/)

While the FedRAMP package provides detailed results of the assessment, the IRS 1075 publication also mandates certain operational and managerial control requirements for agencies wishing to migrate workloads to cloud. In this whitepaper we explore these cloud specific requirements to enable agencies to understand how VMware Cloud on AWS GovCloud (US) can support agencies in meeting IRS 1075 mandatory cloud requirements.

**VMware Cloud on AWS GovCloud (US)**

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.

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).

![Software Defined Data Center (SDDC)](image)

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.

VMware Cloud on AWS GovCloud (US) also offers an optional disaster recovery service called VMware Site Recovery (VSR). VMware Site Recovery for VMware Cloud on AWS GovCloud (US) enables agencies to protect and migrate their workloads to FedRAMP compliant AWS GovCloud regions in the US. The service automates workload recovery in a disaster recovery event between on-premises data centers and VMware Cloud on AWS GovCloud (US), as well as...
between different instances of VMware Cloud on AWS. Built on top of enterprise-grade disaster recovery tools (VMware Site Recovery Manager, vSphere Replication) and the AWS GovCloud (US) regions, the service provides an end-to-end disaster recovery solution that is quick to deploy and leverages existing skills and knowledge of disaster recovery.

**Mandatory requirements for FTI in a cloud computing environment**

IRS 1075 prescribes mandatory controls for all cloud service and deployment models. To utilize a cloud computing model to receive, transmit, store or process FTI, the agency must comply with all IRS 1075 publication requirements. The following mandatory requirements are in effect for introducing FTI to a cloud environment:

<table>
<thead>
<tr>
<th>IRS 1075 cloud computing mandatory requirement</th>
<th>How VMware Cloud on AWS GovCloud (US) supports the requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FedRAMP authorization</strong></td>
<td>VMware Cloud on AWS GovCloud (US) is FedRAMP Authorized at the High impact level. FedRAMP 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 FTI in the VMware Cloud on AWS GovCloud (US) region. For more details on the VMware Cloud on AWS GovCloud (US) region see <a href="https://www.vmware.com">VMware Cloud on AWS GovCloud (US)</a></td>
</tr>
<tr>
<td><strong>Onshore access</strong></td>
<td>The VMware Cloud on AWS GovCloud (US) service is deployed in AWS data centers in the AWS GovCloud US-WEST and US-EAST regions which are physically located in the United States. The service is operated by VMware employees who are U.S citizens on U.S soil. VMware employees do not need access to FTI to operate either the VMware Cloud on AWS GovCloud (US) service or the VMware Site Recovery (VSR) service. Access to customer content (virtual machines, operating systems, applications, file systems or FTI) on GovCloud is solely governed by customer’s use of authentication and authorization mechanisms to secure access to VMs, applications and filesystems that hold their data.</td>
</tr>
<tr>
<td><strong>Physical description</strong></td>
<td>The VMware Cloud on AWS GovCloud (US) service is deployed in AWS data centers in the AWS GovCloud US-WEST and US-EAST regions which are physically located in the United States. AWS does not disclose the actual location of the data centers. Agencies are responsible for selecting the appropriate region when deploying the SDDC to restrict the location of information processing, information/data, and/or information system services to organization-defined locations based on organization-defined requirements or conditions. For more details on AWS data centers please see <a href="https://aws.amazon.com">AWS Global Infrastructure</a></td>
</tr>
<tr>
<td>IRS Publication 1075 cloud computing mandatory requirement</td>
<td>How VMware Cloud on AWS GovCloud (US) supports the requirement</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **45 Day notification**  
The agency must notify the IRS Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment. | Agencies can utilize the *Cloud Computing Notification Form* provided by the IRS Office of Safeguards to notify them 45 days prior to transmitting FTI to the VMware Cloud on AWS GovCloud (US) platform. VMware can support agencies with providing information necessary to complete the notification form, such as for assistance on completing the notification form contact your VMware Account Representative. |
| **Data isolation**  
Software, data and services that receive, transmit, process or store FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications. | VMware Cloud on AWS GovCloud (US) customer environments are both logically and physically isolated in the following three ways:  
1. VMware Cloud on AWS GovCloud (US) has independent and comprehensive isolation layers in place to segregate customers’ environments. A Software Defined Data Center (SDDC) is deployed in a dedicated AWS Virtual Private Cloud (VPC) that is owned by an AWS Account created exclusively for each customer. Amazon Accounts and Amazon VPC’s are the mechanisms implemented by AWS to logically isolate sections of the AWS Cloud for each customer.  
2. VMware Cloud on AWS GovCloud (US) leverages bare metal servers from AWS to provide each customer with dedicated physical server hardware used to build each VMware cluster.  
3. All customer data imported to VMware Cloud on AWS GovCloud (US) is stored on dedicated physical hardware, including dedicated local self-encrypting self-encrypting NVME drives. The Self-Encrypting Drives (SED) use AWS 256-bit XTS encryption.  
Each customer is responsible to encrypt and protect the customer content contained in their tenant space. As part of the shared responsibility model, customers are responsible for securing their sensitive data with in-guest encryption and/or application encryption software that may offer options for alternative key management systems to enable full control of the key management lifecycle. |
| **Service Level Agreements (SLA) and Contracts**  
The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled and accessed inside the cloud through a legally binding contract or SLA with their third-party cloud provider. | The VMware Cloud on AWS GovCloud (US) Service Description describes how FTI is stored, handled and accessed. The Service Description can be accessed via *VMware Cloud on AWS GovCloud Service Description* |
<table>
<thead>
<tr>
<th>IRS 1075 cloud computing mandatory requirement</th>
<th>How VMware Cloud on AWS GovCloud (US) supports the requirement</th>
</tr>
</thead>
</table>
| **Data encryption in transit**  
FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA. | VMC on AWS GovCloud protects the confidentiality and integrity of transmitted information. All data in transit is encrypted using a FIPS 140-2 validated ciphers. VMC on AWS GovCloud currently supports the use of TLS 12 in the VMC on AWS GovCloud SaaS environment.  
For customer connections, TLS 12 is utilized both at the vSphere UI and VMC Console interfaces.  
Within the VMC on AWS GovCloud boundary, encryption of data occurs in transit and at rest within the AWS GovCloud, which ensures that federal data and metadata that is transmitted between AWS instances, and stays within the authorization boundary, is encrypted using FIPS-validated algorithms. AWS provides secure and private connectivity between EC2 instances and automatically encrypts traffic between I3en instances in the same VPC. |
| **Data encryption at rest**  
FTI must be encrypted while at rest in the cloud using a NIST-validated, FIPS 140-2 compliant encryption module. Encryption protects the confidentiality and integrity of the data and provides a methodology for segmenting an agency’s data from others while stored. This requirement must be included in the SLA. | VMware Cloud on AWS GovCloud SDDCs provide storage for customer data at rest using VMware vSAN technology which is configured to encrypt data at rest using a FIPS 140-2 validated XTS-AES 256 algorithm.  
Storage for data at rest in customer SDDCs is provided by VMware vSAN and is implemented as a ‘Workload Datastore’. The Workload Datastore is controlled by the customer owned cloud administrator account and is available to store workload VMs, folders, templates, and ISO images. For additional details please see vSAN Encryption in VMware Cloud on AWS. |
| **Persistence of data in relieved assets**  
Storage devices where FTI has resided must be securely sanitized and/or destroyed using methods acceptable by National Security Agency/Central Security Service (NSA/CSS). This requirement must be included in the SLA. | As part of the shared responsibility model, media sanitization is handled by AWS. Multiple levels of encryption with independent keys are in place to handle media sanitization before repurposing of any hardware. Upon the explicit deletion of an SDDC by a customer, a cryptographic wipe of the vSAN Datastores is performed via destruction of the encryption keys used in the SDDC. For additional details please see vSAN Encryption in VMware Cloud on AWS.  
At the physical hardware layer AWS has implemented policies and procedures for storage end of life. When a physical storage device has reached the end of its useful life, a decommissioning process that is designed to prevent FTI from being exposed to unauthorized individuals is followed using techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process. For additional details see articles on AWS Data Protection. |
<table>
<thead>
<tr>
<th>IRS 1075 cloud computing mandatory requirement</th>
<th>How VMware Cloud on AWS GovCloud (US) supports the requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessments</td>
<td>Agencies must include VMware Cloud on AWS GovCloud (US) in their risk assessments. VMware can provide information necessary to support the risk assessments such as audit reports and security questionnaire responses. VMware Cloud on AWS GovCloud (US) also undergoes regular external audits to demonstrate compliance with US public sector requirements, for more information on audits and compliance see <a href="#">VMware Cloud on AWS GovCloud (US) Roadmap</a>.</td>
</tr>
<tr>
<td>Multi-factor authentication</td>
<td>Customers are responsible for implementing multi-factor authentication for the major system components, including: VMware Cloud on AWS GovCloud Console, SDDC management components including vCenter Server and NSX Manager, and any customer deployed Virtual Machines. For details on configuring federated authentication please refer to the <a href="#">Onboarding Guide</a>. The VMware Government Operations team utilizes FIPS validated multifactor authentication tokens to access VMware Cloud on AWS control plane services. All operations users are issued a FIPS 140-2 certified hard token to authenticate to the service.</td>
</tr>
<tr>
<td>Security control implementation</td>
<td>Agencies can leverage the VMware Cloud on AWS GovCloud (US) FedRAMP package to conduct their own security assessments. VMware’s FedRAMP package can be requested via the FedRAMP PMO by completing a Package Access Request Form and submitting it to <a href="mailto:info@fedramp.gov">info@fedramp.gov</a>, or by contacting their VMware Sales Account Manager. VMware has also published a System Security Plan (SSP) which details the controls implemented to meet the FedRAMP requirements. Agencies can use this information to verify the security control implementation in line with IRS 1075 requirements and their own organizational policies.</td>
</tr>
</tbody>
</table>

Risk assessments
The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing and transmitting FTI. The IRS Office of Safeguards will evaluate the risk assessment as part of the 45 Day notification requirement.

Multi-factor authentication
Cloud implementations which truly represent remote access from the internet must incorporate multi-factor authentication.

Security control implementation
Customer defined security controls must be identified, documented and implemented. The customer defined security controls, as implemented, must comply with Publication 1075 requirements.
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 taxpayer information and provide agencies and the IRS confidence to host their 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 tax agencies to meet IRS 1075 requirements. This whitepaper provides an overview of our measures to meet these 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

- Matt Dreyer – Senior Director, Product Management, VMware Cloud Solutions
- Patrick O’Brien – Group Product Line Manager, VMware Cloud Solutions
- Moin Nawaz Syed – Product Line Manager, VMware Cloud Solutions
Protecting access to customer data