FIRST DRAFT

CLOUD COMPUTING MISSION OWNER SECURITY REQUIREMENTS GUIDE OVERVIEW

Version 1, Release 0.2

21 August 2023

Developed by DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Cloud Computing Mission Owner Security Requirements Guide (SRG) provides the technical security policies and requirements for applying security concepts to the DOD Mission Owner's cloud computing environment. It is designed to work in conjunction with the Cloud Service Provider SRG, which contains guidance that is targeted more toward Cloud Service Providers (CSPs). Missions above Secret must follow existing applicable DOD policies and are not covered by this SRG.

Mission Owners are program managers within the DOD Components responsible for creating instances of enclaves, platforms, or applications by leveraging a CSP's cloud service offerings (CSOs). Within the cloud service environment, one or more instances of devices, networks, and platforms may exist. The Mission Owner is responsible for selecting CSP offerings that are approved in accordance with the Cloud Computing SRG and have a DOD Provisional Authorization (PA).

It is important to understand the division of responsibility between the organization and the CSP. For a traditional physical infrastructure, the organization is responsible for securing the whole stack, including the network security devices, the operating system (OS), and the application. However, as cloud services are integrated, some aspects of the security model shift to the CSP, while others are the responsibility of the Mission Owner. The responsibility for security is thus different depending on whether the cloud service selected is an enclave, a platform, or a software application and may vary within each service provider's offering. It is crucial that consumers of these various offerings have a detailed understanding of the delineation of duties between themselves and CSPs for each offering. However, for all cloud deployment types, DOD retains security configuration and protection responsibilities for securing any data that cannot be released to the public.

1.1.1 Security Requirements Guides (SRGs)

Security Requirements Guides are collections of requirements applicable to a given technology family. They represent an intermediate step between Control Correlation Identifiers (CCIs) and Security Technical Implementation Guides (STIGs). CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in a policy, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product's technology area.

There are four core SRGs: Application, Network, Operating System, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, Technology SRGs are developed to address the technologies at a more granular level.

This Cloud Computing Mission Owner SRG is based on the Operating System and Network SRGs. The Cloud Computing Mission Owner SRG contains general check and fix information that can be used for products for which STIGs do not exist.

The STIGs based on this SRG will provide the product-specific technical implementation guidance for that product. The STIG will contain the specific check and fix information for the product it covers.

SRG Hierarchy example:

Application SRG
|__*Database SRG*
|__*Microsoft SQL Server 2016 STIG*

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and to provide appropriate justification. It also provides the structure to identify variations in specific values based on the technology family. These variations will be captured once and will propagate down to the Technology SRGs and then to the STIGs. This will eliminate the need for each product-specific STIG to address items that are not applicable.

1.1.2 SRG Naming Standards

To establish consistency across the SRGs, a naming standard for the Group Title and STIGIDs has been established.

Technology SRG Naming Standards

For Technology SRG Group Title and STIGIDs, the following applies:

{*Core SRG value*}-{*Technology SRG*}-{*5- or 6-digit numeric sequence number*}

Examples:

SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
SRG-NET-000001-VVSM-00001
SRG-OS-000001-UNIX-000001

Checks/fixes will be included at this level in a general form. These checks and fixes will apply for any STIGs that are created for products that do not have product-specific check and fix guidance.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the

National Security Agency (NSA)/Central Security Service (CSS), using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems Instruction (CNSSI) 1253.

1.2.1 Relationship to STIGs

The SRG defines the requirements for various technology families, and the STIGs are the technical implementation guidelines for specific products. A single SRG/STIG is not all-inclusive for a given system, which may include but is not limited to Database, Web Server, and Domain Name System (DNS) SRGs/STIGs. For a given system, compliance with all (multiple) SRGs/STIGs applicable to a system is required.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 SRG and STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 NIST SP 800-53 Requirements

All applicable baseline technical NIST SP 800-53 requirements and security best practice requirements are included in this SRG.

CNSSI 1253 defines the required controls for DOD systems, based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

2.2 General Procedures

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured system. These procedures are not product specific and are intended for use when a product-specific STIG is not available.

2.3 Security Assessment Information

A documented Service Level Agreement (SLA) must delineate the responsibility for security between the CSP and the Mission Owner. The exact delineation depends on how the CSP implements the security features it supports in the CSO and additional services the Mission Owner has contracted to add.

The Mission Owner will use the Department of Defense Information Network (DODIN) and other DOD infrastructure, including the Cloud Access Points (CAPs) or DOD Cybersecurity Service Provider (CSSP). Therefore, many settings/requirements in the Cloud Computing Mission Owner SRG and other DISA STIGs will not be applicable or configurable by the Mission Owner. In this case, the reviewer will ensure these functions are in place and mandated by the SLA between the applicable organizations.

The Cloud Computing Mission Owner SRG addresses only overarching cloud environment requirements that in some instances may not be covered as part of the PA.

- The Network Infrastructure STIG is required as part of any cloud enclave Infrastructure as a Service (IaaS) assessment.
- Applicable network device STIGs or SRGs are required as part of the cloud enclave assessment or where any network-level device is configured or third-party contracted by the Mission Owner and not part of the PA.
- To secure the instances of the operating systems and applications installed by the Mission Owner, the applicable operating system and application STIGs must be part of the assessment.
- For hardening Software as a Service (SaaS), the appropriate application STIG may be required but is usually considered accomplished via the cloud service's PA.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

The following sections focus on Mission Owner requirements. CSO requirements are more thoroughly discussed in the Cloud Service Provider SRG.

3.1 Types of Cloud Implementations

The CAP architecture will change character depending on whether the cloud infrastructure is on-premises or off-premises. There are internal CAPs (ICAPs) and DODIN/NIPRNet/SIPRNet Boundary CAPs (BCAPs). Refer to the Cloud Computing Services Provider SRG, section 5.9.1, for additional information.

Off-premises CSOs are commercial data centers, systems, and CSPs operating within facilities that are not under the direct control of the DOD. On-premises CSOs include DOD data centers, authorized commercial data centers, other facilities located on a DOD Base, Camp, Post, and Station (B/C/P/S), or in a commercial or another government facility (or portions thereof) under the direct control of DOD personnel and DOD security policies.

For the on-premises cloud, the Mission Owner is responsible for security of all cloud components, including the physical hosting hardware. Security configuration and hardening is very similar to a traditional network environment. The Mission Owner must comply with DOD requirements for the entire security stack, including the cloud network security devices, operating systems, applications, and authentication services.

3.1.1 IaaS

With the cloud-based enclave or IaaS, the CSP is responsible for the physical hosting hardware. The Mission Owner must comply with DOD requirements for the entire security stack, including the cloud network security devices, operating systems, applications, and authentication services.

3.1.2 PaaS

In the case of a PaaS, the CSP is responsible for the security of the cloud-based hardware and the operating system that make up the platform. The Mission Owner does not manage or control the underlying cloud infrastructure of the platform, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Some minor controls of network security services such as a web application firewall, antivirus, and authentication servers may be owned or shared depending on the service used. Application components not provided by the CSP platform are usually installed and/or configured by the Mission Owner because this type of service often supports software development environments. Detailed configuration of the operating system environment is not in scope and requires use of the applicable operating system to fully secure it prior to installation of applications or DOD files.

3.1.3 SaaS

In the case of SaaS, the CSP is responsible for the security of the cloud-based hardware, virtual machine (VM) environment, operating system, and application. Application use policy is configured by the Mission Owner because this type of service is the purchase of a particular application. Occasionally, SaaS offerings may provide some low-level security controls to Mission Owners that must be clearly documented in an SLA application.

3.2 CSP/CSO Approval Process

The DOD Chief Information Officer (CIO) allows DOD components to acquire cloud services directly from commercial CSPs or privately from DISA or other federal agencies. Each component remains responsible for determining what data and missions are hosted by external cloud service providers.

Each use of cloud services must be analyzed using the Enterprise IT Business Case Analysis (BCA) template. The BCA must be approved by the CSSP and Mission Owner Approving Authority. DISA provided cloud services must be considered as part of the BCA. Federal Risk Authorization and Management Program (FedRAMP) Moderate is the minimum-security baseline for non-National Security Systems (NSSs), FedRAMP High is the requirement for NSS and Classified Information up to Secret for DOD cloud services. Components and Mission Owners may host Unclassified DOD information that has been publicly released on FedRAMP Moderate approved cloud services.

A CSO that meets these additional requirements is granted a DOD PA that allows a non-DOD CSP to host DOD missions. A DOD PA provides a validation of a CSP's compliance with DOD guidance for hosting systems operating at an indicated DOD System Impact Level.

3.3 Mission Owner Responsibilities

Mission Owners are entities such as program managers within the DOD Components who are responsible for instantiating information systems and applications by using a CSP's CSO. Mission Owners initiate the process by selecting either a DOD CSP or a non-DOD CSP to host their cloud service. They then work with their designated authorizing officials and complete the RMF accreditation. This process must follow their organizations designated path to the cloud.

In addition to complying with the requirements in the Cloud Computing Mission Owner SRG, the Mission Owner is responsible for the following:

- Completing the actions required to obtain an Authority to Operate (ATO) for their mission systems/applications.
- Register the protocols and services along with their related UDP/TCP IP Ports used by the SaaS service that will traverse the DODIN in the DOD PPSM registry. This includes all user and management plane traffic for Impact Levels 4, 5, and 6 as well as management plane traffic for level 2 if managed/monitored from within a DOD network.
- Registering the Mission Owner's system/service/application with the DOD whitelist for both inbound and outbound traffic.

- Registering the CSP's CSO in System/Network Approval Process (SNAP) for the connection approval, which also includes designating a certified CSSP as the Defensive Cyberspace Operations (DCO).
- Collaborating with CSSP during cloud architecture development to ensure required security relevant data will be accessible via CSP/CSO, third-party security service subscription, and/or native API capability.
- Serving as DCO for their mission systems/applications.
- Ensuring CSP requirements for DCO, component, and other requirements, with particular attention to data ownership and legal jurisdiction, are included in the cloud contract/SLAs (e.g., component/service requirements for incident handling and reporting). Requirements are located in Section 3.3.7 and in the Cloud Service Provider SRG (section 5.2 and chapter 6).
- Data spill security processes and procedures must be clearly defined and addressed in the contract/SLAs with the CSP (CNSSP 32).

3.3.1 SaaS Mission Owner Responsibilities

For the SaaS cloud offering, the CSP is responsible for security of the software service itself, the Mission Owner remains responsible for the security of their DOD data and any configuration settings that are within the control of the Mission Owner. The Mission Owner must register the services as indicated in the previous section. There must be a clear delineation of responsibility for security between the CSP and the Mission Owner.

Mission Owners operate applications that are provided by the CSO under SaaS. The entirety of the security stack (i.e., from the physical network through the application layers) is the responsibility of the vendor.

The exact delineation of responsibility may shift depending on the specifics for the cloud service. The Mission Owner maintains the requirement to secure their data and identity management. The provider may bundle security in whole or as part of the Mission Owner selecting this service as an add-on component. The Mission Owner must register the services as indicated in the previous section.

As stated in the general requirements in the previous section, Mission Owners must collaborate with the CSSP during cloud application development/procurement. This will ensure that appropriate security service subscriptions are part of the build to gain access to required security-relevant data.

3.3.2 IaaS/PaaS Mission Owner Security and Architecture Responsibilities

For cloud enclaves (i.e., IaaS), the Mission Owner is responsible for securing the guest operating systems, the applications they build, and the cloud network on which these systems operate. The CSP remains responsible for securing the hypervisors, servers, storage, and physical networks.

Mission Owners build systems and applications on cloud infrastructure provided by the CSO under IaaS/PaaS. Data flows within and between cloud networks and platforms, as well as to external networks, must flow through a security stack and have logical separation as required for all DOD networks. There must be a clear delineation of responsibility for security between the CSP and the Mission Owner.

For cloud platforms (i.e., PaaS), the Mission Owner is responsible for ensuring the security of the guest operating systems and the platform applications they build. The exact delineation of responsibility may shift depending on the specifics for the cloud service. The provider may bundle security in whole or as part of the Mission Owner selecting this service as an add-on component. Document the clear delineation of responsibility for the CSO in the SLA.

Mission Owner cloud enclave and platform responsibilities include but are not limited to ensuring the following architecture and devices are configured and approved:

- DOD DMZ Extension – Implement cloud network(s) in accordance with the approved architecture for the type of application as defined in the DOD DMZ STIG and the Application Security and Development STIG, along with other operating system and application-specific STIGs. For example, a web service or application is typically required to have unrestricted/restricted DMZ zones with appropriate protections for internet/externally facing servers and private/"back-end" zones with appropriate protections for application/database servers and other supporting systems/servers.
- Virtual Datacenter Security Stack (VDSS) – A VDSS provides enclave security capabilities such as firewall, intrusion detection, and intrusion prevention systems. It also provides application security capabilities such as Web Application Firewall (WAF) and proxy systems. The VDSS can reside within or outside of the CSP's infrastructure (cloud-based or physically). VDSS capabilities can also be provided as a service by a third-party vendor (for IaaS) or a CSP (for IaaS and SaaS). VDSS feeds must be provided to a DOD CSSP performing enclave boundary defense.
- Virtual Datacenter Managed Service (VDMS) – VDMS is designed to provide endpoint protections for Mission Owner applications such as DOD ACAS, host based/endpoint security solution, IDAM, etc. It provides system management network and Mission Owner cloud enclave/platform/OS support services that form the management plane. VDMS provides secure management network connectivity between the Defense Information Systems Network (DISN), cloud host-based management services, and identity and access management services for DOD Common Access Card (CAC) authentication to cloud systems. The VDMS is specifically tailored to operate at all DOD mission Impact Levels. VDMS functionality applies directly to IaaS environments but may not be specifically applicable to PaaS and SaaS CSOs as such functionality may be inherent to the associated CSP and validated through the DOD PA.
- Cloud Storage – Implement FIPS 140-2/3 compliant, data-at-rest encryption on all DOD files housed in CSP IaaS storage service offerings. The Mission Owner may choose from one or more CSP offerings or methods to accomplish this.
- Host-Based/Endpoint Security – Implement a host-based security suite to monitor servers and endpoints that complies with DOD regulations and Component needs. Ensure there is a secure (encrypted) connection or path between the endpoint security agents and their control server.
- Vulnerability Scanning – Implement scanning using a vulnerability scanner that complies with DOD regulations and Component needs.

- DOD CAC/PKI – Implement a secure (encrypted) connection or path between the implemented systems/applications and the DOD Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) resources on NIPRNet or SIPRNet as applicable.
- Active Directory (AD) (if used) and any associated trusts IAW the DOD Windows OS STIGs and/or other applicable DOD STIGs – This includes trusts between DOD Active Directory (AD) forests and CSP CSO AD forests. If such trusts are required, the implementation must be approved by the AO responsible for the DOD AD forest.
- VM OS – Configure IAW the applicable OS STIG.
- CSP-provided applications – Configure IAW the appropriate Application STIG. Applies to applications provided by the CSP under PaaS.
- Mission Owner applications – Configure IAW the appropriate Application STIG.

3.3.3 Choosing the Information Impact Level

The current cloud Security Model categorizes information into Impact Levels 2, 4, 5, and 6. These levels combine the type of information to be stored and processed in the CSP environment and the potential impact of an event that results in the loss of confidentiality, integrity, or availability of DOD data, systems, or networks. When making an assessment, the Mission Owner must emphasize the integrity and availability of the information to show that the cloud implementation will achieve a level of security and risk acceptable to the responsible AO. While the Mission Owner may choose a higher level to process data from a lower level of information, DISA recommends organizations select cloud services based on appropriate risk levels.

Risk management includes risk assessment, mitigation, and documentation of residual risk. In a cloud environment, the system/applications inherit both the security controls that the CSP implements for their organization/facilities and the residual risk of the CSO. Refer to Section 4 of the Cloud Service Provider SRG for guidance on Mission Owner risk assessment and authorization boundaries.

The following discussion is focused on a general summary of the architecture for each impact level.

- Impact Level 2: Non-Controlled Unclassified Information.
- Impact Level 4: Controlled Unclassified Information.
- Impact Level 5: Controlled Unclassified Information requiring additional protection, including unclassified National Security Systems (NSSs).
- Impact Level 6: Classified Information up to Secret.

Impact Level 2 has minimal requirements for confidentiality. User connectivity to the information system flows through the CSP's internet connection; thus, DOD is relying on the network boundary protections and monitoring that the CSP provides for all customers versus capabilities normally provided by a DOD CSSP. Protection that supports the cloud-based enclave/application/host will be provided by a combination of the CSP protections and the Mission Owner's cloud-based datacenter's security management stack.

Impact Level 4, 5, and 6 data presents greater risk and requires enterprise defense mechanisms and data collection that enable robust monitoring, event correlation, and analytics. The DODIN boundary is essentially extended through a connection between the DOD CAP and the CSP's network infrastructure supporting the DOD mission. Therefore, an event may be detected by different entities: the CSP through monitoring of their CSO (especially for SaaS); the mission administrators or owners; or the CSSP that is supporting the monitoring of the mission and the boundary connection. All entities must work together to quickly investigate and respond to incidents. This change requires new constructs within the Defensive Cyber Operations (DCO) Command and Control (C2) structure, including the identification of entities with new DCO C2 and Operations (Ops) responsibilities. The use of a CAP drives the requirement for two distinct functions/roles: DODIN Boundary DCO and Mission. Refer to the Cloud Computing Servers Provider SRG paragraph 5.9.1 for additional information.

Impact Level 6 data contains Classified up to Secret. The architecture essentially is an extension of the SIPRNet. Only DOD private, DOD community, or Federal Government community clouds that are standalone or connected to Secret networks (e.g., SIPRNet) are eligible for Impact Level 6.

3.3.4 Encryption of Data-at-Rest in Commercial Cloud Storage

Mission systems at all Impact Levels must have the capability for DOD data to be encrypted at rest with exclusive DOD (Mission Owner) control of encryption keys and key management. Some CSOs may facilitate this by providing a Hardware Security Module (HSM) or offering customer-dedicated HSM devices as a service. CSOs that do not provide such a capability may require Mission Owners to use encryption hardware/software on the DISN or a cloud encryption service that provides DOD control of keys and key management. Some CSOs may offer a Key Management System (KMS) service that can suffice for management of customer keys by the customer while preventing CSP access to the keys (NIST 800-53 Rev 5 SC-12(6)). It is recommended that such CSP KMS services be evaluated by NSA.

Data-at-rest encryption with Mission Owner-controlled keys and key management protects the DOD data stored in CSOs with the following benefits:

- Maintains the integrity of publicly released information and websites at Impact Level 2 where confidentiality is not an issue.
- Maintains the confidentiality and integrity of CUI at Impact Levels 4/5 with the following benefits:
  - Limits the insider threat vector of unauthorized access by CSP personnel through increasing the work necessary to compromise/access unencrypted DOD data.
  - Limits the external threat vector of unauthorized access by hackers through increasing the work necessary to compromise/access unencrypted DOD data.
  - Enables high-assurance data destruction for CSP offboarding through cryptographic erasure and file deletion without CSP involvement or cooperation.
  - Enables high-assurance data spill remediation through cryptographic erasure and file deletion without CSP involvement or cooperation.

Mission Owners and their AOs should consider the benefits of DAR encryption for data destruction and/or spill remediation at Impact Level 2 in addition to the benefit of maintaining integrity of the information.

For all Information Impact Levels:

- Encrypt all data at rest:
  - Stored in VM virtual hard drives.
  - Stored in mass storage facilities/services whether at the block or file level.
  - Stored in database records (whether PaaS or SaaS where the Mission Owner does not have sole control over the database and database management system).
- Use FIPS 140-2 or FIPS 140-3 validated cryptography modules (minimally Level 1) operated in FIPS mode in accordance with federal government policy/standards for the protection of all CUI.
  - Cryptography modules include cryptographic algorithm, RNG, KMI, HASH, etc. (all approved functions).
- CSP Mission Owner maintains control of the keys, from creation through storage and use to destruction.
  - Implement Hardware Security Modules (HSM) or Key Management Servers as needed to store, generate, and manage keys within the DISN; or
  - Order a CSP service that provides a dedicated HSM that is managed solely by the MO; or
  - Order a CSP KMS service that has been evaluated by NSA.

For cloud applications where encrypting data at rest with DOD key control is not possible, Mission Owners must perform a risk analysis with relevant data owners before transferring data into a CSO. This analysis must consider a high-assurance method may not be available to remediate data spills or ensure destruction of data at the application's end of life and CSO offboarding. Mission Owner AOs are responsible for accepting these risks.

The DAR encryption capabilities of CSP CSOs, and ability to support Mission Owners' DAR encryption requirements, will be assessed and documented toward the award of the DOD PA.

3.3.4.1 Cryptographic Erase

Cryptographic erase is an emerging sanitization technique that can be used in some situations when data is encrypted as it is stored on media. With CE, media sanitization is performed by sanitizing the cryptographic keys used to encrypt the data, as opposed to sanitizing the storage locations on media containing the encrypted data. Cryptographic erase techniques are typically capable of sanitizing media very quickly and could support partial sanitization, a technique where a subset of storage media is sanitized. Partial sanitization, sometimes referred to as selective sanitization, has potential applications in cloud computing.

Data-at-rest encryption, coupled with exclusive Mission Owner control of cryptographic key management, provides DOD the ability to cryptographically erase data at rest without CSP assistance or cooperation. Data deletion refers to normal file or data record deletion methods used in file systems and databases. Deletion before or after cryptographic erase will restore resources to the CSP and permit the eventual overwriting of the data under normal operations. To support cryptographic erase and the various benefits it provides, data-at-rest encryption must be performed at an appropriate level of granularity. This means that one key should not be used to encrypt all or large chunks of Mission Owner data.

Related Security Controls: MP-6(3), MP-6(8)

3.3.5 Overlays

CNSSI 1253 overlays may be required based on the level of the information system. All appropriate overlays must be addressed. The current DOD Risk Management Framework Technical Advisory Group values, CNSSI 1253 values, or AO tailored values must be used.

3.3.6 Additional FedRAMP+ Security Control

The additional NIST 800-53 Rev 5 security controls will be addressed by the Mission Owner, the CSP, or both. The parameters will be the DOD RMF Technical Advisory Group (TAG) value, the CNSSI 1253 value if no DOD RMF TAG value exists, or the AO tailored value unless designated by this document.

Table 3-1: FedRAMP+ Security Control

Control	Parameter Values	Impact Level
AC-7	For privileged users, DOD limits to three unsuccessful attempts and requires an administrator to unlock. For nonprivileged users, if rate limiting, DOD will allow 10 attempts with the account automatically unlocked after 30 minutes. If rate limiting is not used, normal DOD Specific Assignment Value (DSPAV) will be required.	IL4, IL5, IL6
AU-5(1)	DSPAV will be used, not FedRAMP.	IL5, IL6
CM-7(5)		IL4, IL5, IL6
MA-5(1)		IL4
MA-5(2)		IL6
MA-5(3)		IL6
MA-5(4)		IL6
MA-5(5)		IL5, IL6
MA-6	DSPAV will be used, not FedRAMP.	
PS-3(4)	All information systems. Users: U.S. citizens, U.S. nationals, or U.S. persons, foreign personnel as allowed by current DOD Polices with AO approval. Administrators: U.S. citizens, U.S. nationals, or U.S. persons.	IL4, IL5, IL6
PS-4	DSPAV will be used, not FedRAMP.	IL4, IL5, IL6
SA-4(5)		IL4
SA-9(1)		L4, IL5, IL6

Control	Parameter Values	Impact Level
SA-9(3)		L4, IL5, IL6
SA-9(5)	SA-9 (5)-1 [information processing, information or data, AND system services] SA-9 (5)-2 [U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction] SA-9 (5)-3 [all data, systems, or services]	IL4, IL5, IL6
SA-9(6)		IL4, IL5, IL6
SA-9(7)		IL4, IL5, IL6
SA-9(8)		IL4, IL5, IL6
SC-12(6)		IL4, IL5, IL6
SC-17	DODI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling	IL4, IL5, IL6
SC-18	DSPAV will be used, not FedRAMP.	IL4, IL5, IL6
SC-24	DSPAV will be used, not FedRAMP.	IL4, IL5, IL6
SC-46		If CDS is used

3.3.7 Contract/SLA Requirements

Table 3-1 above shows the security controls designated for potential inclusion in a Mission Owner's contract or SLA with the CSP. All the controls listed are baseline requirements for NSS (IL5/IL6), and AC-02(13) is the baseline requirement for Impact Level 4. The Mission Owner may tailor the contents of the contract or SLA to include any of the controls in Table 3-2 beyond the FedRAMP and DOD Baseline and FedRAMP+ security controls. The Mission Owner is responsible for defining any parameter values associated with any added security control. These values should be based on current DOD RMF TAG values or CNSSI 1253 values.

While these security controls generally address system availability, they apply to the availability of information related to continuous monitoring, incident response, and other security issues. This listing does not preclude the Mission Owner from addressing any control or enhancement from any CNSSI 1253 baseline or the NIST SP 800-53 rev5 in the contract/SLA if they need to tailor the control/enhancement to be provided/met by the CSP to secure their system or application. Assessment and continuous monitoring of compliance with these security controls is the responsibility of the Mission Owner as negotiated with the CSP in attaining and maintaining the mission's Authority to Operate. Not all of these security controls are assessed currently toward the award of a DOD PA.

Table 3-2: Security Controls to be Addressed in the Contract/SLA

SP 800-53r4 Cont./Enh. ID	Level 4	Level 5	Level 6
AC-02 (13)	X	X	X
AC-03 (04)	X	X	X

SP 800-53r4 Cont./Enh. ID	Level 4	Level 5	Level 6
AC-12 (01)		X	X
AC-16	X	X	X
AC-16 (06)	X	X	X
AU-10		X	X
IA-03 (01)	X	X	X
PS-04 (01)	X	X	X
PS-06 (03)	X	X	X
SC-07 (11)	X	X	X
SC-07 (14)	X	X	X
SC-18 (03)		X	X
SC-18 (04)		X	X
Total	**9**	**13**	**13**

The Mission Owner for CSP Personnel must address NIST 800-53 Rev 5 controls PS-3(4), Personnel Screening Citizenship Requirements, for Impact Levels 4/5/6 in the contract with the values of assignment: all information types and citizenship requirements: U.S. citizen, U.S. nationals, or U.S. persons. No foreign persons may have such access.

Access to DOD information at the various levels above Impact Level 2 is limited by national affiliation. For other than U.S. citizens or noncitizen U.S. nationals as defined in 8 U.S. Code § 140857, national affiliation is defined in 22 CFR 120.1558 – U.S. person and 120.16 – foreign person.

- 8 U.S. Code § 1408: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title8/pdf/USCODE-2010-title8-chap12-subchapIII-partI-sec1408.pdf
- 22 CFR 120.15, 120-16: https://www.gpo.gov/fdsys/pkg/CFR-2011-title22-vol1/pdf/CFR-2011-title22-vol1-sec120-15.pdf

The Contract/SLA must address data spillage, data ownership including legal jurisdiction, mobile code, facilities, and personnel requirements discussed in the Cloud Service Provider SRG, Section 5 and subsections.

The Contract/SLA must address incident response requirements discussed in the Cloud Service Provider SRG, Section 6 and subsections.

The Mission Owner must ensure the contract/SLA specifies that the DOD shall have the authority to conduct Penetration Testing on all Impact Level 6 CSP offerings at any time of its choosing using methods of its choosing.