DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

Version 1, Release 2

18 March, 2016

Developed by the
Defense Information Systems Agency
for the
Department of Defense

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 DoD, DISA, the DISA Risk Management Executive (RME), or DISA RME Cybersecurity Standards Branch of any non-Federal entity, event, product, service, or enterprise.

Table of Contents

List of Tables

List of Figures

This page is intentionally blank.

1 INTRODUCTION

Cloud computing technology and services provide the Department of Defense (DoD) with the opportunity to deploy an Enterprise Cloud Environment aligned with Federal Department-wide Information Technology (IT) strategies and efficiency initiatives. Cloud computing enables the Department to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. The overall success of these initiatives depends upon well executed security requirements, defined and understood by both DoD Components and industry. Consistent implementation and operation of these requirements assures mission execution, provides sensitive data protection, increases mission effectiveness, and ultimately results in the outcomes and operational efficiencies the DoD seeks.

The 15 December 2014 DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services* defines DoD Component responsibilities when acquiring commercial cloud services. The memo allows components to responsibly acquire cloud services minimally in accordance with the security requirements outlined in Federal Risk and Authorization Management Program (FedRAMP) and this Cloud Computing Security Requirements Guide (CC SRG). Defense Information Systems Agency (DISA) previously published the concepts for operating in the commercial cloud in the *Cloud Security Model*. Version 1 defined the overall framework and provided initial guidance for public data. Version 2.1 added information for Controlled Unclassified Information. The CC SRG documents cloud security requirements in a construct similar to other SRGs published by DISA for the DoD. This SRG incorporates, supersedes, and rescinds the previously published Cloud Security Model.

The following terms will be used throughout this document:

- **Cloud Service Provider (CSP):** refers to any or all Cloud Service Providers, DoD or non-DoD.
- **Non-DoD CSP:** will refer to a commercial or Federal Government owned and operated CSP.
- **Commercial CSP:** will refer to a Non-DoD Non-Federal Government organization offering cloud services to the public and/or government customers as a business, typically for a fee with the intent to make a profit.
- **DoD CSP**: will refer to a DoD owned and operated CSP (e.g., milCloud).
- **Cloud Service Offering (CSO)**: refers to a CSP's product or service offering recognizing that a CSP may have multiple product/service offerings, e.g., Microsoft O-365 and Azure.
- **DoD Cloud Service Catalog:** The repository of all CSOs that have been awarded DoD PAs and have security packages available for DoD components to leverage.
- **DoD Component:** The DoD Services and Agencies and their sub command organizations
- **Mission Owner:** While DoD Components are the owners of all IT missions under their purview, for the purpose of this SRG and other DoD Cloud guidance, the term Mission Owner refers to entities such as IT system/application owner/operators or program managers within the DoD Components/Agencies responsible for instantiating and operating one or more information systems and applications who may leverage a CSP's CSO in fulfilment of IT missions. In this context the Mission Owner is not the DoD Enterprise or DoD Component/Agency Enterprise even though these entities may control

and have oversite for Component/Agency level policies and Mission Owner's acquisitions. The Mission Owner is also the Data/Information Owner. The data owner, in addition to owning the data/information and all associated derivatives, is responsible for ensuring the data that is migrated to the cloud is at the appropriate security level.

- **C/CEs** (Control/Control Enhancements): National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Security and Privacy controls and their enhancements which are selected and assembled in various baselines and overlays.
- **Provisional Authorization (PA):** See Section 2.6 - *DoD Provisional Authorization.*

1.1 Purpose and Audience

This CC SRG outlines the security model by which DoD will leverage cloud computing along with the security controls and requirements necessary for using cloud-based solutions.

The CC SRG serves several purposes:

- Provides security requirements and guidance to DoD and commercial CSPs that wish to have their CSO(s) included in the DoD Cloud Service Catalog[1].
- Establishes a basis on which DoD will assess the security posture of a DoD or non-DoD CSP's CSO, supporting the decision to grant a DoD PA that allows a CSP to host DoD missions.
- Establishes a basis on which a DoD Component's Authorizing Official (AO) will assess the security posture of a DoD CSP's CSO, supporting the decision to grant a DoD Component's Authorization to Operate (ATO) for the CSP/CSO, and a DoD PA if the CSO might be leveraged by other DoD Components. (e.g., DISA's ATO/PA for milCloud)
- Defines the requirements and architectures for the use and implementation of DoD or commercial cloud services by DoD Mission Owners.
- Provides guidance to DoD Mission Owners and officials , Security Control Assessors, Authorizing Officials, (formerly Certification and Accreditation (C&A) officials), and others in planning and authorizing the use of a CSO.
- Supports the DoD CIO's Cloud initiative to migrate DoD web sites and applications from physical servers and networks within DoD networks and data centers into lower cost commodity IT services which typically include virtual servers and networks that are an integral part of most cloud services provided by both DoD and commercial CSPs.
- Supports the DoD CIO's and Federal Government's Data Center Reduction initiatives.

The audience for this CC SRG includes:

- Commercial and non-DoD Federal Government CSPs
- DoD programs operating as a CSP
- DoD Components and Mission Owners using, or considering the use of, commercial/non-DoD and DoD cloud computing services
- DoD risk management assessment officials and Authorizing Officials (AOs)

[1] DoD Cloud Service Catalog:
https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx (DoD CAC/PKI required)
http://www.disa.mil/~/media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf (Public)

1.2 Authority

This document is provided under the authority of *DoD Instruction 8500.01* and *DoD Instruction 8510.01*.

DoD Instruction (DoDI) 8500.01, entitled *Cybersecurity*, directs Director DISA, under the authority, direction, and control of the DoD CIO to develop and maintain 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 Central Security Service (NSA/CSS), using input from stakeholders, and using automation whenever possible.

DoDI 8500.01 further directs DoD Component heads to ensure that all DoD IT under their purview comply with applicable STIGs, [NSA] security configuration guides, and SRGs with any exceptions documented and approved by the responsible AO.

DoDI 8510.01 implements *NIST Special Publication (SP) 800-37, NIST SP 800-53, Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253,* and the *Federal Information Security Management Act (FISMA)* by establishing the DoD Risk Management Framework (RMF) for DoD IT, establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF.

1.3 Scope and Applicability

DoDI 8510.01, para 2a states: “This instruction applies to: (2) All DoD IT that receive, process, store, display, or transmit DoD information. These technologies are broadly grouped as DoD IS, platform IT (PIT), IT services, and IT products. This includes IT supporting research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD.”

DoDI 8510.01, Encl 3, para 3b (page 13) defines internal and external IT Services (formerly "Outsourced IT-based Processes"). Cloud computing by its nature fits this definition which is as follows:

> "3b. IT Services. IT services are outside the service user organization's authorization boundary, and the service user's organization has no direct control over the application or assessment of required security controls. DoD organizations that use IT services are typically not responsible for authorizing them (i.e., issue an authorization decision).
>
> (1) Internal IT services are delivered by DoD ISs. DoD organizations that use internal IT services must ensure the categorization of the IS delivering the service is appropriate to the needs of the DoD IS using the service, and that written agreements describing the roles and responsibilities of both the providing and the receiving organization are in place.
>
> (2) DoD organizations that use external IT services provided by a non-DoD federal government agency must ensure the categorization of the IS delivering the service is appropriate to the confidentiality, integrity, and availability needs of the information and mission, and that the IS delivering the service is operating under a current authorization from that agency. In accordance with Reference (h) [ed. DoDI 8500.01], interagency agreements or government statements of work for these external services must contain requirements for service level agreements (SLAs) that include the application of appropriate security controls.

> (3) DoD organizations that use external IT services provided by a commercial or other non-federal government entity must ensure the security protections of the IS delivering the service is appropriate to the confidentiality, integrity, and availability needs of the DoD organization's information and mission. DoD organizations must perform categorization in accordance with Reference (e) [ed. CNSSI 1253] and tailor appropriately to determine the set of security controls to be included in requests for proposals. DoD organizations will assess the adequacy of security proposed by potential service providers, and accept the proposed approach, negotiate changes to the approach to meet DoD needs, or reject the offer. The accepted security approach must be documented in the resulting contract or order.
>
> (4) DoD organizations contracting for external IT services in the form of commercial cloud computing services must comply with DoD cloud computing policy and procedural guidance as published."

This CC SRG, in support of DoDI 8510.01, Encl 3, para 3b, establishes the DoD security objectives to host DoD mission applications and DoD information in internal and external IT services in the form of CSP's CSOs. The sensitivity of the DoD information may range from publicly releasable up to and including SECRET. Missions above SECRET must follow existing applicable DoD and Intelligence Community (IC) policies and are not covered by this CC SRG.

NOTE: The IC offers approved Cloud Services at classification levels above SECRET. Contact the DoD CIO Cloud team for additional information at: osd.cloudcomputing@mail.mil.

This CC SRG applies to all CSPs/CSOs hosting DoD systems/information/data/applications, regardless of who owns or operates the environments. Owners/operators can be DoD Components, Federal Government agencies, or commercial entities.

This CC SRG supports the responsibilities of DoD Component heads, per 44 USC 3534 (a) (1) (ii) (Federal Information Security Management Act (FISMA)), to provide protections for "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency". CSPs not operated by the Mission Owner are essentially "a contractor of an agency" which operates an information system on "behalf of an agency". Mission Owners contracting with a CSP are outsourcing all or a portion of their information technology workloads to the CSP. This is the same as the use of "IT services" under DoDI 8510.01, Encl 3, para 3b.

This CC SRG also applies to all DoD mission owners using cloud services and all parties involved in the provisioning of cloud services to DoD mission owners. This includes integrators or brokers and CSPs serving as prime contractor as well as any supporting CSP or facilities provider (i.e., sub-contractor) that an integrator/broker/CSP might leverage or contract with to provide a complete service or set of services under a DoD contract. For example, if CSP A instantiates their SaaS offering in CSP B's IaaS offering, which is located in CSP C's data center, the CC SRG is applicable to all three CSP/CSO entities for the applicable requirements. Similarly, for a cloud services integrator/broker which uses or resells one or more CSPs/CSOs to full contract requirements, the CC SRG is applicable to all cloud services. While the CSP's overall service offering may be inheriting controls and compliance from a third party, the prime CSP, the CSP with a DoD contract for service, is ultimately responsible for complete compliance. This applicability statement and associated requirements are consistent with DoD and Federal acquisition requirements and clauses which state that DoD contractors, in this case integrators/brokers/CSPs must include all security requirements incumbent upon them in all subcontracts.

The authorization process for commercial and non-DoD CSPs is based on FISMA and NIST RMF processes through the use of FedRAMP, supplemented with DoD considerations as outlined in Section 4, *Risk Assessment Of Cloud Service Offerings* of this document. These requirements and considerations are a subset of the requirements in the DoD RMF. The authorization process for DoD enterprise service programs providing cloud capabilities or service offerings (e.g. milCloud, Defense Enterprise Email) is based on the DoD RMF requirements and processes which are similar to the FISMA and NIST RMF processes. Both processes utilize similar baselines of the NIST SP 800-53 security controls as the basis of the assessment, providing a common framework under which DoD can determine the level of risk.

This SRG establishes the DoD baseline security requirements for DoD Mission Owners when contracting for and using non-DoD Software as a Service (SaaS) offering, and when implementing their systems and applications on DoD or non-DoD Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings. Since IaaS and PaaS involve CSP customers building a system or application on top of these service offerings, this release of this CC SRG considers IaaS and PaaS as being similar and treats them in the same manner, unless stated otherwise. SaaS is addressed to the extent of the other service models, with specific application requirements being identified in other application-related SRGs and STIGs.

NOTE: Recognizing that PaaS CSOs can range from very close to IaaS where the mission owner is only provided with a few unsecured programming environments and an OS that the Mission Owner must secure to very close to SaaS where the CSO is a mostly complete application that mission owner can only customize its interface, PaaS will be better addressed in a future release of this CC SRG.

NOTE: While this CC SRG applies to all DoD use cases of cloud computing, one of the primary focus points of this SRG is to facilitate the migration of DoD systems and applications hosted on physical infrastructure (virtualized or not) owned by DoD Components and connected to DoD Defense Information System Network (DISN) services (i.e., Non-secure Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet) to DoD or non-DoD Cloud Services (as defined by NIST. See Section 2.1, *Cloud Computing, Cloud Service, and Cloud Deployment Models* for this definition). This SRG does not address all DoD systems and applications unless they are migrating to or leveraging DoD or non-DoD Cloud Services nor does it address approved DoD or non-DoD systems and applications used by DoD that are already approved for direct access via the Internet (not traversing the DISN) unless they are migrating to commercial cloud services directly accessed via the Internet. While this SRG may be used to assess/approve such cloud services and the applications that use them, it is not intended to change the approved network access or connectivity methods they use.

1.4 Security Requirements Guides (SRGs) / Security Technical Implementation Guides (STIGs)

Security Requirements Guides (SRGs) are collections of security requirements applicable to a given technology family, product category, or an organization in general. SRGs provide non-product specific requirements to mitigate sources of security vulnerabilities commonly encountered across IT systems and applications.

While the SRGs define the high level requirements for various technology families and organizations, the Security Technical Implementation Guides (STIGs) are the detailed guidelines

for specific products. In other words, STIGs provide product-specific information for validating, attaining, and continuously maintaining compliance with requirements defined in the SRG for that product's technology area.

A single technology related SRG or STIG is not all inclusive for a given system. Compliance with all SRGs/STIGs applicable to the system is required. This typically results in a given system being subject to multiple SRGs and/or STIGs.

Newly published SRGs and STIGs generally consist of a technology/product overview document and one or more eXtensible Markup Language (XML) (.xml) files in Extensible Configuration Checklist Description Format (XCCDF) containing the security requirements. Security requirements are presented in the form of Control Correlation Identifiers (CCIs) and include product specific configuration and validation procedures. Requirements in this CC SRG are not being published in an XCCDF XML format at this time.

The security requirements contained within SRGs and STIGs, in general, are applicable to all DoD-administered systems, all systems connected to DoD networks, and all systems operated and/or administrated on behalf of the DoD. This requirement remains in force for all Mission Owners building systems in a cloud service. CSP systems must comply with configuration guidance consistent with the NIST SP 800-53 control CM-6 by utilizing STIGs/SRGs or a configuration guide deemed equivalent by DoD.

1.5 SRG and STIG Distribution

Interested parties can obtain the applicable SRGs and STIGs from the Information Assurance Support Environment (IASE) website. The unclassified website is http://iase.disa.mil and the classified website is http://iase.disa.smil.mil.

NOTE: Some content requires a DoD Public Key Infrastructure (PKI) certificate for access. The IASE web site does NOT currently accept External Certificate Authority (ECA) certificates for entry into the PKI-protected area. Industry partners needing PKI restricted content may request it through their DoD sponsor.

1.6 Document Revisions and Update Cycle

DISA Risk Management Executive, Cybersecurity Standards Branch develops, revises, updates, and publishes SRG and STIG documents on a quarterly maintenance release schedule as needed. These publications reflect new or changed policies, requirements, threats, or mitigations; reorganized content; corrected errors; and/or, to provide additional clarity. The fiscal year based release schedule can be found at http://iase.disa.mil/stigs/Pages/fso-schedule.aspx.

Major updates to an SRG or STIG result in a version change rather than an incremental release. New SRGs and STIGs and major updates will be released as soon as they are approved and ready for publication at any time during the year.

1.6.1 Comments, Proposed Revisions, and Questions

Comments, proposed revisions, and questions are accepted at any time via email at disa.stig_spt@mail.mil.

DISA Risk Management Executive, Cybersecurity Standards Branch coordinates all change requests with relevant DoD organizations before inclusion and subsequent publication in a maintenance release or major update.

1.7 Document Organization

This SRG is organized into six major sections with supporting appendices. Sections 1-4 address general information including the processes for authorizing a particular CSP's cloud offering. Remaining sections outline specific security requirements to be addressed in authorizing and operating cloud capabilities. In addition to specifics on SRG roles and responsibilities and required control parameter values, the appendices provide the references and definitions used throughout the document.

Section 1, *Introduction*: Provides general information on the purpose and use of this document.

Section 2, *Background*: Contains a primer on several terms and supporting concepts used throughout the document.

Section 3, *Information Security Objectives / Impact Levels*: Explains the concept of "Information Impact Levels" based on the type of data being hosted in the cloud and outlines security objective considerations in the areas of Confidentiality, Integrity, and Availability.

Section 4, *Risk Assessment of Cloud Service Offerings*: Provides an overview of the RMF processes used for granting a DoD PA and explains how a PA can be leveraged by a Mission Owner and its AO in support of an ATO decision.

Section 5, *Security Requirements*: Details the requirements associated with enabling CSP capabilities.

Section 6, *Cyber Defense and Incident Response*: Outlines the requirements for defending information systems operating in the cloud along with the Command and Control (C2) processes necessary to defend and operate DoD mission systems.

This page is intentionally blank.

2 BACKGROUND

This section outlines several concepts, terms, and supporting processes, providing a primer for the remainder of this document.

2.1 Cloud Computing, Cloud Service, and Cloud Deployment Models

NIST SP 800-145[2] defines cloud computing as having five essential characteristics, three service models, and four deployment models. This SRG adheres to these NIST definitions to characterize and standardize the discussion of Cloud Computing. Cloud Computing is defined as follows:

> "**Cloud computing** is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The Essential Characteristics are:

> **"On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
>
> **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
>
> **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
>
> **Rapid elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
>
> **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.**"**

The NIST defined cloud service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) and are defined as follows:

> **"Software as a Service (SaaS).** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or

[2] NIST SP 800-145: http://csrc.nist.gov/publications/PubsSPs.html

control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). "

NIST defines cloud deployment models as follows.

"**Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). "

This SRG uses private and community to mean the following: "DoD private/community cloud" refers to a cloud service that is built for the exclusive use of DoD users or tenants. "Federal Government Community cloud" is one that includes both DoD and other Federal Government tenants. For example, a cloud used exclusively by Army and Air Force tenants would be considered DoD private/community, while one utilized by DISA and the Department of State would be a Federal Government community cloud.

While vendors may market and name their offerings as they wish, DISA will categorize them into one of the three NIST cloud service models when listing them in the DoD Cloud Service Catalog. Vendors are encouraged to market their services using the NIST cloud service model terminology. Service offerings that provide data storage without also providing computing services will be considered to be a subset of IaaS. Furthermore any other service models proposed by the vendor (such as Data as a Service (DaaS)) will have to be aligned to one the three standard service delivery models and meet the appropriate controls. As used in this SRG

the terms cloud computing and cloud services refer to a service offering from a provider organization to one or more organizational customers or tenant organizations. These terms do not refer to classic forms of IT services delivery where dedicated hardware (whether it is virtualized or not) is employed or assembled by organizations for their own use. A service offering from a provider organization to a customer must be part of the construct.

2.2 Cloud Service Provider (CSP) and Cloud Service Offering (CSO)

A Cloud Service Provider (CSP) is an entity that offers one or more cloud services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third party facilities such as data centers, carrier hotels / collocation facilities, and Internet Exchange Points (IXPs)). CSPs offering SaaS may leverage one or more third party CSO's (i.e., for IaaS or PaaS) to build out a capability or offering.

A Cloud Service Offering (CSO) is the actual IaaS/PaaS/SaaS solution available from a CSP. This distinction is important since a CSP may provide several different CSOs.

2.3 DoD Risk Management Framework (DoD RMF)

DoDI 8510.01 is the implementing policy for the DoD RMF, establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. This DoD policy is consistent with NIST SP 800-37, Guide for Applying the Risk Management Framework, which defines RMF for the Federal Government. CNSSI 1253 and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations are incorporated into this DoD policy, which outline the controls and control baselines used in the assessment process. Of critical importance to this SRG, DoDI 8510.01 "provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs)."

2.4 Federal Risk and Authorization Management Program (FedRAMP)

The Federal Risk and Authorization Management Program[3], or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the Federal Government. The use of FedRAMP is mandated for all Federal Agencies by the Office of Management and Budget (OMB) as their systems and applications are migrated to the commercial cloud under the Federal Government's Cloud-First initiatives. The December 2011 OMB FedRAMP policy memo[4] requires Federal departments and agencies to utilize FedRAMP approved CSPs and share Agency ATOs with the FedRAMP Secure Repository.

FedRAMP uses a "do once, use many times" framework that intends to reduce cost, time, and staff required for security assessments and process monitoring reports. The FedRAMP Joint Authorization Board (JAB) is the primary governance and decision-making body for the

[3] FedRAMP: https://www.fedramp.gov/
[4] December 2011 OMB Policy Memo: https://www.fedramp.gov/files/2015/03/fedrampmemo.pdf

FedRAMP program. JAB-approved standards and processes result in the award and maintenance of a PA to host Federal Government missions.

DoD leverages FedRAMP JAB PAs and non-DoD U.S. Government Federal Agency ATO packages residing in the FedRAMP Secure Repository, including all supporting documentation when assessing a CSO for a DoD PA. However, DoD will only accept non-DoD Agency ATOs where the CSP/CSO was assessed by a FedRAMP accredited Third Party Assessor Organization (3PAO).

NOTE: The American Association for Laboratory Accreditation[5] (A2LA) accredits FedRAMP 3PAOs with the FedRAMP Program Management Office (PMO) providing final approval.

2.5 FedRAMP Plus (FedRAMP+)

FedRAMP+ is the concept of leveraging the work done as part of the FedRAMP assessment, and adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements. A CSP's CSO can be assessed in accordance with the criteria outlined in this SRG, with the results used as the basis for awarding a DoD provisional authorization.

2.6 DoD Provisional Authorization

A DoD Provisional Authorization (PA) is an acceptance of risk based on an evaluation of the CSP's CSO and the potential for risk introduced to DoD networks. The DoD PA process follows the same "do once, use many times" framework as FedRAMP does. DoD PAs are granted at all information impact levels. A PA provides a foundation that AOs responsible for mission applications must leverage in determining the overall risk to the missions/applications that are executed as part of a CSO.

Since all CSOs offered by a CSP may not have been submitted for assessment, a DoD PA is granted to the CSP for a CSO, not the CSP itself. Furthermore, if a CSP's CSO leverages another CSP's CSO (e.g., CSP A instantiates their SaaS offering in CSP B's IaaS offering) then the DoD PA for CSP A's CSO includes inherited compliance of CSP B. In this case, CSP A will be contractually responsible for CSP B and must have accountability for controls in their sub-contracts. It is therefore highly recommended that CSPs offering service to DoD only utilize other CSOs that have a DoD PA. In the event a leveraged CSP/CSO does not have a PA, it will be assessed as part of the prime CSO. Such subtended assessments will not automatically grant the leveraged CSP/CSO an independent PA. CSPs must disclose subcontracted CSOs used in the CSOs offered to DoD when assessed for a DoD PA.

NOTE: DoD PAs are not granted to physical facilities by themselves (e.g., a data center) that support cloud infrastructure even if it might be considered a CSO if the facility supports multiple CSPs or multiple tenants' equipment. These are assessed for the physical and environmental controls as part of the CSP's CSO by the 3PAO for unclassified facilities. Classified processing facilities are addressed later in this CC SRG.

A DoD PA is revocable in the event a CSP/CSO loses its FedRAMP PA or if the CSP does not maintain compliance with its security responsibilities identified in this CC SRG, associated requirements found in other referenced documents, or contract requirements. Additionally, a

[5] American Association for Laboratory Accreditation: https://www.a2la.org/

CSP's CSO with a DoD PA which leverages another CSP's CSO with a DoD PA may lose their PA if the leveraged CSO loses its PA. CSPs acting as prime contractor must maintain the PA for their CSO and require all sub contracted CSPs to maintain the PA for their CSOs for the term of the contract. This flow-down is also applicable to cloud services integrators and brokers acting as prime contractors. If a prime or subcontracted CSO losing a PA and refuses to correct or cannot correct the reason(s) for it, such a condition may constitute a breach of contract. While revoking a PA is an extreme measure, DoD will work with the CSP to resolve the issues leading to revocation. Consistent with the December 2014 DoD CIO Memo,[6] the DISA AO is responsible for approving and revoking DoD PAs.

CSOs possessing a DoD PA are listed in the DoD Cloud Service Catalog[7]. DoD Component services may also implement approved CSP/CSO listings for their agency's use.

[6] Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services: http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20CIO%20-%20Updated%20Guidance%20-%20Acquisition%20and%20Use%20of%20Commercial%20Cloud%20Serviices_20141215.pdf

[7] DoD Cloud Service Catalog:
https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx (DoD CAC/PKI required)
http://www.disa.mil/~/media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf (Public)

This page is intentionally blank.

3 INFORMATION SECURITY OBJECTIVES / IMPACT LEVELS

Cloud security information impact levels are defined by the combination of: 1) the sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and 2) the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information. DoD Mission Owners must categorize mission information systems in accordance with DoDI 8510.01 and CNSSI 1253 then identify the Cloud Information Impact level that most closely aligns with the defined categorization and information sensitivity. The Cloud Information Impact Levels are further defined in Section 3.2, *Information Impact Levels.*

3.1 Security Objectives (Confidentiality, Integrity, Availability)

Information Impact Levels consider the potential impact should the confidentiality or the integrity of the information be compromised.

According to Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*,[8] confidentiality is "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542][9]. A loss of confidentiality is the unauthorized disclosure of information.

FIPS Publication 199 defines integrity as "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information. It is important to note that the unauthorized destruction of information will result in the loss of availability of that information.

FIPS-199 defined three levels to designate the impact of a loss of confidentiality or a loss of integrity (refer to Table 1). The security control baseline for all Impact Levels is based on moderate confidentiality and moderate integrity. If a Mission Owner has high potential impacts, specific requirements must be included in the contract/SLA to address/mitigate this risk or deploy to DoD facilities assessed using CNSSI 1253 high baselines through the DoD RMF. In the future DISA will consider incorporating a FedRAMP High Baseline into this SRG after one becomes available.

[8] FIPS 199: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
[9] 44 U.S.C., Sec. 3542: http://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

Table 1 - Potential Impact Definitions for Security Objectives (FIPS-199)

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

While the FedRAMP baseline addresses availability, the DoD Cloud baseline objectives do not additionally address the impact of availability; it is expected that the Mission Owner will assess the CSO's stated availability rating(s) during CSP selection. Any specific or additional availability requirements must be included in the contract or a service level agreement with the CSO. Mission Owners must ensure the language is specific and inclusive for their required availability. For example, if the requirement is "CSP maintenance affecting system availability must be coordinated 4 weeks in advance and shall not exceed 4 hours per month," then the contract / SLA should detail the requirement. Recommended contract / SLA availability controls are provided under the FedRAMP+ Controls/Enhancements in Section 5.1.6, *Security Controls/Enhancements to be optionally addressed in the Contract/SLA.*

CSOs will be evaluated as part of the assessment process for availability. The assessed level of availability will be listed in the DoD Cloud Service Catalog. This evaluation does not prevent a CSO from receiving a PA or being included in the DoD Cloud Service Catalog; it is only used to facilitate the matching of a DoD Mission Owner to one or more appropriate cloud services meeting their needs.

3.2 Information Impact Levels

The previously published (and now superseded) Cloud Security Model[10] defined 6 information Impact Levels. In order to simplify the selection process, the number of levels was reduced from 6 to 4. This was accomplished by integrating levels 1 (public information) and 3 (low impact CUI) into levels 2 and 4, respectively. The numeric designators for the Impact Levels have not been changed in order to remain consistent with previous versions of the Cloud Security Model,

[10] Cloud Security Model: http://iase.disa.mil/cloud_security/Pages/archive.aspx

leaving Impact Levels 2, 4, 5, and 6. Note that a higher level can process data from a lower level.

Additionally, the security control baseline used to assess CSP CSOs for a PA for all levels has been changed to moderate confidentiality and moderate integrity as defined by CNSSI 1253 and the FedRAMP Moderate Baseline. This modification for Impact Levels 5 and 6 from high confidentiality and high integrity is intended to better align with the categorization of most DoD customer systems that will be deployed to commercial CSP facilities. Mission owners with systems categorized at high confidentiality or integrity impact levels must deploy to facilities assessed using CNSSI 1253 high baselines through the DoD RMF (typically a DoD facility) or contract for the added security from a commercial CSP. DISA will consider incorporating a FedRAMP High Baseline into this SRG after one becomes available.

Figure 1 provides a summary of the current information impact levels coupled with some of the distinguishing requirements and characteristics.

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

NOTE: See Section 5.2.1, *Jurisdiction/Location Requirements* for the explanation of "US / US outlying areas".
NOTE: ADP-1 and ADP-2 Personnel Requirements apply to both impact levels 4 and 5.
NOTE: Level 4/5 off-premises CSO connectivity will be via a CAP on any DISN network (e.g., DREN) it serves.

Figure 1 – Impact Level Comparison

The following subsections describe the impact levels, to include those used previously, and the type of information to be stored or hosted in CSOs by Mission Owners.

3.2.1 Level 1: Unclassified Information approved for Public release

Level 1 is no longer used and has been merged with Level 2.

3.2.2 Level 2: Non-Controlled Unclassified Information

Level 2 includes all data cleared for public release, as well as some DoD private unclassified information not designated as Controlled Unclassified Information (CUI) or critical mission data, but the information requires some minimal level of access control. This level accommodates Non-CUI information categorizations based on CNSSI-1253 up to low confidentiality and moderate integrity (L-M-x).

3.2.3 Level 3: Controlled Unclassified Information

Level 3 is no longer used and has been merged with Level 4.

3.2.4 Level 4: Controlled Unclassified Information

Level 4 accommodates CUI or other mission critical data. CUI is information the Federal Government creates or possesses that a law, regulation, or Government-wide policy requires, or specifically permits, an agency to handle by means of safeguarding or dissemination controls. CUI requires protection from unauthorized disclosure as established by Executive Order (EO) 13556, Controlled Unclassified Information (November 2010)[11], Part 2002 of 32 CFR[12], the CUI Registry [13]and DoDM 5200.01, Vol 4[14], which is currently being updated. CUI does not include classified information, or information a non-executive branch entity possesses and maintains in its own systems that did not come from an executive branch agency or entity acting for an agency. Designating information as CUI or critical mission data to be protected at Level 4 is the responsibility of the owning organization. Determination of the appropriate impact level for a specific mission with CUI and mission data will be the responsibility of the mission AO. Some types of CUI may not be eligible to be hosted on Impact Level 4 and 5 CSOs without a specific rider to the DoD PA. (e.g., for Privacy.) This level accommodates CUI information categorizations based on CNSSI-1253 up to moderate confidentiality and moderate integrity (M-M-x)

CUI contains a number of categories[15], including, but not limited to the following:

- Export Controlled--Unclassified information concerning items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. This includes dual use items; items identified in Export Administration Regulations (EAR)[16], International Traffic in Arms Regulations (ITAR)[17] and the munitions list; license applications; and sensitive nuclear technology information.

[11] EO 13556: https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
[12] Part 2002 of 32 CFR: https://www.gpo.gov/fdsys/granule/CFR-1998-title32-vol6/CFR-1998-title32-vol6-part2002
[13] CUI Registry: https://www.archives.gov/cui/registry/category-list.html
[14] DoDM 5200.01, Vol 4: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf
[15] CUI Categories: http://www.archives.gov/cui/registry/category-list.html
[16] Department of Commerce EAR: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear
[17] Department of State ITAR: https://www.pmddtc.state.gov/regulations_laws/itar.html

- Privacy Information--Refers to personal information or, in some cases, *personally identifiable information* (PII)[18] as defined OMB M-07-16[19] or *means of identification* as defined in 18 USC 1028(d)(7)[20].
- Protected Health Information (PHI)[21] as defined in 45 C.F.R. §160.103)[22].
- Other information requiring explicit CUI designation (i.e., For Official Use Only, Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information).

3.2.5 Level 5: Controlled Unclassified Information

Level 5 accommodates CUI that requires a higher level of protection than that afforded by Level 4 as deemed necessary by the information owner, public law, or other government regulations. Level 5 also supports unclassified National Security Systems (NSSs) due to the inclusion of NSS specific requirements in the FedRAMP+ C/CEs. As such, NSS must be implemented at Level 5. Some types of CUI may not be eligible to be hosted on Impact Level 4 and 5 CSOs without a specific rider to the DoD PA. (e.g., for Privacy.) This level accommodates NSS and CUI information categorizations based on CNSSI-1253 up to moderate confidentiality and moderate integrity (M-M-x).

3.2.6 Level 6: Classified Information up to SECRET

Level 6 accommodates information that has been determined: "(i) pursuant to EO 12958, *Classified National Security Information* (April 17, 1995) as amended by EO 13292[23], or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, (P.L. 83-703)[24] to be Restricted Data (RD)." At this time, only information classified as SECRET or below, in accordance with the applicable EOs, is permitted to be hosted at this level. This level accommodates classified information categorizations up to moderate confidentiality and moderate integrity (M-M-x).

[18] NIST SP 800-22, Protecting PII: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
[19] OMB M-07-16: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
[20] USC 1028: http://www.gpo.gov/fdsys/granule/USCODE-2010-title18/USCODE-2010-title18-partI-chap47-sec1028
[21] PHI: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/
[22] 45 C.F.R. §160.103: http://www.ecfr.gov/cgi-bin/text-idx?SID=fdaad816fa8b26001747e9fb198429be&mc=true&node=se45.1.160_1103&rgn=div8
[23] EO 12958 as amended by EO 13292: http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html
[24] AEA 1954 as amended: http://pbadupws.nrc.gov/docs/ML1327/ML13274A489.pdf#page=23

This page is intentionally blank.

4 RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS

The shift to cloud computing necessitates adjustments to the DoD Risk Management processes, which typically address physical on-premises systems and applications, to accommodate the use of commercial CSOs. The goal is to address the security requirements and controls, relative to the criticality of DoD information in the cloud, in a cost effective and efficient manner, while still assuring the security of DoD's core missions and networks in accordance with the DoD RMF. To support the relationship of missions to cloud capabilities, DoD has defined information Impact Levels (discussed in Section 3.2, *Information Impact Levels*) that broadly align to the criticality and sensitivity of data, and missions that would operate in a cloud environment. The DoD PA risk assessment process is focused on evaluating the requirements for the impact level(s) which a CSP's CSO is capable of supporting. When choosing a CSP's CSO, the mission owner must pick a CSO that fits their operational needs and that possesses a DoD PA at the information impact level corresponding to the categorization of the information to be processed or stored in the CSO. The PA and supporting documentation must then be leveraged by the Mission Owner's Authorization Official in granting the required ATO for the mission system operating within the cloud.

NOTE: For the purpose of the CC SRG, the use of the term "Assessment and Authorization (A&A)" refers to the collection of RMF processes which includes "Security Control Assessment, Risk Assessment (informed by Security Control Assessment), Ongoing Assessment (continuous monitoring), and System Authorization.

4.1 Assessment of Commercial/Non-DoD Cloud Services

The 15 December 2014 DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services,* states "components may host Unclassified DoD information that **has been publicly released** on FedRAMP approved cloud services." The memo also states "FedRAMP will serve as the minimum security baseline for all DoD cloud services."

***Impact Level 2*:** Using the definitions outlined in Section 3.2, Impact Level 2 information may be hosted in a CSP that is government assessed as FedRAMP compliant at the moderate level. The two acceptable government assessments include:

- JAB PA – Based on a determination by the JAB that an acceptable level of risk exists for leveraging across the Federal Government. DoD is an active participant in the technical reviews of the JAB PA security assessment artifacts.
- FedRAMP listed Agency ATOs – Based on an assessment and ATO issued by a Federal Government agency where the CSP was assessed by a FedRAMP accredited/approved 3PAO.

DoD will not perform additional assessments at Level 2 before awarding a DoD PA and listing in the DoD Cloud Service Catalog[25].

[25] DoD Cloud Service Catalog:
https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx (DoD CAC/PKI required)
http://www.disa.mil/~/media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf (Public)

Impact Level 4/5: Assessments for Impact Levels 4 and above are based on a combination of the security controls in the FedRAMP Moderate baseline and the DoD specific controls/requirements outlined in Section 5.1.2, *DoD FedRAMP+ Security Controls/Enhancements* and throughout this SRG. Where possible, DoD leverages documentation and artifacts from previous FedRAMP-JAB or non-DoD Agency authorizations in the FedRAMP Secure Repository and additional CSP proprietary artifacts provided by the CSP. FedRAMP+ requirements will be assessed by a FedRAMP accredited/approved 3PAO. An overall determination of risk is prepared by the DISA Cloud Security Control Assessor (SCA) organization to support a DoD PA decision. The DISA AO (formerly the DISA DAA) approves DoD PAs.

There are three paths that can be followed in assessing a CSP for a Level 4/5 DoD PA and subsequent listing in the DoD Cloud Service Catalog[26] available to DoD personnel. These are:

- **CSPs with a FedRAMP JAB PA or in the process of obtaining a JAB PA:** DoD leverages the documentation and artifacts produced as part of the FedRAMP process, supplemented with an assessment of the DoD-specific security controls and requirements not addressed by FedRAMP for Impact Levels 4 and above. CSPs having a FedRAMP JAB PA have been assessed by an accredited/approved 3PAO against the FedRAMP Moderate Baseline. For those in the process of obtaining a JAB PA, DoD promotes the use of parallel activities (FedRAMP and FedRAMP+) to minimize cost and create efficiencies in the assessment process.
  NOTE: This is the DoD preferred path to a DoD PA because the DoD SCA and the DoD CIO have already been involved in the assessments and authorization activities.

- **FedRAMP listed Non-DoD Agency ATO:** CSPs having a non-DoD Federal agency authorization based upon security controls assessed by an accredited/approved 3PAO can be assessed for a DoD PA provided that the authorization is accepted and listed in the FedRAMP agency authorizations. The information from the non-DoD agency ATO will be supplemented with an assessment of the DoD-specific controls and requirements. This additional assessment should be performed by the CSP's 3PAO and submitted to the DISA SCA for review toward awarding a PA.
  NOTE: Mission Owners, their AOs, and/or the DISA SCA need to carefully assess Agency ATOs as the non-DoD agency may have accepted risks that are not appropriate for DoD to accept.

- **DoD Component Assessed PA:** The CSP's CSO is fully assessed, independent of the FedRAMP PMO, by a FedRAMP accredited/approved 3PAO (highly recommended), the DISA Cloud SCA organization, or other approved DoD SCA organization** in coordination with the DISA Cloud SCA organization. The CSP's CSO must be assessed against both the FedRAMP Moderate Baseline and FedRAMP+ requirements.

  When a FedRAMP PA or 3PAO assessed non-DoD Agency ATO does not exist, a DoD Component assessment of a CSP's CSO may only be performed under two circumstances. These are:

[26] DoD Cloud Service Catalog:
https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx (DoD CAC/PKI required)
http://www.disa.mil/~/media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf (Public)

1. If a DoD organization has a validated mission requirement that only the specific CSP's CSO can fulfill requiring it to be authorized, or
2. If a DoD organization acting as a CSP develops and instantiates a CSO.

The DoD organization with a need for that CSP's CSO to be authorized will be required to support resourcing for the full assessment, in coordination with the DISA cloud security assessment team. This assessment of the FedRAMP, FedRAMP+ security controls, and other SRG requirements determines whether to grant a DoD PA and the appropriate impact levels.

If a CSP receives a DoD assessed PA and that service offering may be leveraged by other Federal Agencies, the CSP's assessment package will be shared with and be available through the FedRAMP secure repository as well as the DoD Cloud Services Catalog. If the service offering will only be used by DoD customers the CSP's assessment package will only be available through the DoD Cloud Service Catalog, since private clouds are ineligible for inclusion in the FedRAMP catalog.

While DoD CSP IaaS/PaaS/SaaS CSOs will be assessed for a full ATO under the DoD RMF to support their approval for connection to the DISN, DoD CSP IaaS/PaaS CSOs will also be assessed for a PA IAW the requirements for commercial CSPs in this SRG. The award of a PA to DoD CSP IaaS/PaaS CSOs enable the Mission Owners AOs to leverage the PA in the same manner as a PA for a commercial CSP toward granting an ATO for the systems and applications built on the CSO. For assessment information for DoD SaaS CSOs see Section 4.2, *Assessment of DoD Cloud Services*.

** "Other approved DoD SCA organizations" include those DoD Component level organizations that routinely perform Security Control Assessment activities in support of the Component's AO. Examples are DISA's Risk Management Executive (RME) Certification and Assessment Division RE5, Navy's Space and Naval Warfare Systems Command (SPAWAR) and Air Force Space Command AFSPC.

CSOs may be assessed for both FedRAMP and DoD requirements simultaneously by the same 3PAO. This permits CSPs to avoid redundancies in assessments when they seek to have a CSO included in both the FedRAMP and DoD Cloud Catalog.

Any change of ownership involving a CSP, whether the primary CSP or an underlying CSP on which a CSO was built, will be reviewed by the DISA AO to assess the impacts and risks associated with the continuation of the DoD PA. Furthermore, DoD CIO, the DISA AO, and Mission Owners must be notified of any potential change of CSP ownership six months before the change occurs to allow for the PA review and for Mission Owners to off-board from the CSP and retrieve their information/data if they desire. Mission Owners must address CSP ownership in their SLAs/Contracts. The major concern for DoD is a sale to a non-US organization.

A CSO with a DoD PA does not eliminate the requirement for a given application using the CSO to have an ATO (or IATT) prior to commencing operations as addressed in Section 4.3.3, *Mission Risk.*

NOTICE: DoD Cloud SCA organizations must be experienced in assessing NIST SP 800-53 C/CE. To standardize the quality of assessments across Cloud SCA organizations and the quality

of DoD PAs for use by all DoD Components and Mission Owners, DoD SCA organizations should become accredited by American Association for Laboratory Accreditation (A2LA)[27] and approved by FedRAMP as a 3PAO[28]. Alternately all assessments leveraged for a DoD PA should be done by a FedRAMP approved 3PAO. Furthermore, since DoD PAs are based on the RMF, CSP CSOs assessed under the outdated DoD Information Assurance Certification and Accreditation Process (DIACAP) using DoDI 8500.2 IA controls do not qualify for a DoD PA as this would break the standardization of the basis for the PA and thereby its quality.

Impact Level 6: Assessment and Authorization of **off-premises** DoD contractor facilities and information systems that process, store, transmit classified information (i.e., Non-DoD commercial CSPs and their Level 6 CSOs) must be performed in conjunction with the National Industrial Security Program (NISP) (as defined in Executive Order 12829[29]) and the Industrial Security Regulation (ISR) (DoD 5220.22-R)[30] in accordance with 48 Code of Federal Regulations (CFR) Subpart 4.4 - Safeguarding Classified Information within Industry[31] and Federal Acquisition Regulations (FAR) section 52.204-2 - Security Requirements[32]. NISP policies are the purview of the Office of the Undersecretary of Defense for Intelligence (OUSD(I)) Industrial Security division and, for DoD, the Defense Security Service (DSS). DoDI 5220.22[33] assigns DoD responsibilities for administration of the NISP IAW E.O. 10865 and 12829 to ensure classified information disclosed to industry is properly safeguarded. NISP responsibilities for DoD components are found in the DoD 5220.22-R and DoDI 5220.22; whereas, commercial CSPs with Level 6 offerings must adhere to the National Industrial Security Program Operating Manual (DoD 5220.22-M) [34]. Together the ISR, NISPOM, and Office of the Designated Approving Authority (ODAA) Process Manual[35] provide guidance.

NOTE: It is the intent of the DoD CIO that all CSPs and CSOs are assessed against the same set of requirements and cyber security control baselines as defined in the DoDI 8510.01- DoD RMF, and CNSSI 1253- Security Categorization and Control Selection for National Security Systems and the CC SRG. Requirements and processes supporting the authorization of off-premise Commercial CSPs and their CSOs for Impact Level 6 will be coordinated with OUSD(I) and DSS as NISP policies and procedures are updated. Updated guidance and requirements for off-premises CSPs and their CSOs for a DoD Level 6 provisional authorization may appear in a future release of the CC SRG.

[27] A2LA: http://www.a2la.org/appsweb/fedramp.cfm
[28] FedRAMP 3PAO approval: https://www.fedramp.gov/participate/3paos/
[29] EO 12829, NISP: http://www.archives.gov/isoo/policy-documents/eo-12829.html
[30] DoD 5220.22-R: http://www.dtic.mil/whs/directives/corres/pdf/522022r.pdf
[31] 48 CFR Subpart 4.4:
https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4-subpart4-4
[32] FAR 52.204-2:
https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf
[33] DoDI 5220.22 NISP: http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf
[34] DoD 5220.22-M, NISPOM: http://www.dss.mil/documents/odaa/nispom2006-5220.pdf
[35] (ODAA) Process Manual:
http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf

4.2 Assessment of DoD Cloud Services and Enterprise Services Applications

DoD operated CSOs (e.g., milCloud IaaS/PaaS) are subject to the same requirements found in this SRG and the same security controls as commercial CSPs. However, DoD CSP programs and services must also follow DoD Risk Management procedures in accordance with DoDI 8510.01, which is based on the full sets of controls and control enhancements listed in CNSSI 1253 commensurate with the service's information categorization. DoD enterprise service programs that might be considered cloud services under the SaaS model (even though they may or may not meet the NIST definition of Cloud, i.e., based on an IaaS/PaaS CSO) (e.g., Defense Enterprise Email (DEE), Defense Collaboration Service (DCS), DoD Enterprise Portal Service (DEPS)), are also subject to the DoDI 8510.01 requirements and CNSSI 1253. Such programs are DoD assessed as noted above and not subject to being assessed through the FedRAMP program and do not share DoD ATOs with the FedRAMP secure repository.

DoD is transitioning to the DoD RMF from the DoD Information Assurance Certification and Accreditation Process (DIACAP). DIACAP is based on a set of DoD defined security controls, not the NIST SP 800-53 security control catalog. Cloud services initiated and authorized under the DIACAP will be assessed and authorized using the RMF in accordance with DoD transition guidance as defined in DoDI 8510.01 or supplemental DoD guidance.

Impact Level 6: Assessment and Authorization of **On-Premises** Level 6 CSOs (i.e., DoD or DoD Contractor managed CSOs in a DoD data center) will be performed by DoD Component SCAs in the same manner as any other SIPRNet enclave, service, or application in accordance with DoD established policies and processes IAW DoD RMF for DoD classified facilities, applications, connection approval, and clearances for DoD and DoD contractor personnel. In conjunction with this A&A the CSO may receive a DoD PA if the CSO will be offered to DoD Components other than the authorizing component and the CSO meets the standards defined in this CC SRG for all CSOs. In the event the on-premises CSO is operated/managed by a commercial CSP or other DoD contractor, the CSP/contractor will be required to have the appropriate facilities clearance and cleared personnel as is the case with any DoD contractor that handles classified information. The details of clearing contractors is well known and beyond the scope of the CC SRG.

To receive a DoD PA, DoD On-Premises Impact Level 6 CSOs will be minimally assessed IAW the FedRAMP Moderate Baseline, the Level 6 FedRAMP+ C/CE and the CNSSI 1253 Appendix F, Attachment 5 *Classified Information Overlay* C/CEs. Such CSOs may need to meet additional CNSSI 1253 C/CE in the baselines associated with the categorization of the information to be processed/stored in the CSO.

NOTE: See Section 5.6.2.2, *CSP Personnel Requirements – PS-3: Background Investigations* under the Level 6 topic for additional requirements related to on-premises contractor- managed CSOs WRT organizational facilities clearances and cleared personnel.

4.3 Cloud Service Offering and Mission Owner Risk Management

Risk management must consider both the CSO and the supported mission (i.e., the Mission Owner's system or application). Each CSO must be granted a DoD PA in order to host DoD mission systems. The PA and supporting documentation will then be used by the Mission Owner's risk management officials as a basis of reciprocity for the controls provided by the CSP, recognizing the controls will vary based on the service model (IaaS, PaaS, SaaS) and could also

vary based on requirements such as privacy or classification controls. Additionally, there are controls that are "shared controls" where both the CSO and the Mission Owner need to address a requirement. The responsible AO leverages the PA information, supplemented with an assessment of the risks within the Mission Owner's responsibility, in granting an authorization to operate.

Understanding the distinction between what's provided and addressed with the CSO versus what's addressed by the Mission Owner is critical to implementing the DoD cloud security requirements as defined in this SRG.

4.3.1 Cloud Computing, Authorization Boundaries

In Cloud Computing, there are two primary Authorization Boundaries. These are generally determined by the division of control between CSP and Mission Owner. (see Figure 2 – Notional Division of Security Inheritance and Risk) and are generally defined as follows:

1. CSP and CSO Authorization Boundary addressed by the FedRAMP and DoD PAs consists of two parts:
    a. The CSP organization, their operating/security policies and procedures, physical facilities, network(s), hardware server platforms, hypervisors, VMs, applications, etc., that serves their corporate network and indirectly supports their CSOs. CSOs inherit the C/CEs that the CSP implements along with any resulting residual risk based on how well the C/CEs are implemented
    b. The CSO includes the infrastructure directly supporting the CSO and the following for each service type:
        - IaaS: includes the network, storage, computing platforms, and hypervisors that compose the IaaS service offering.
        - PaaS: may build on the devices and platforms or constructs used in IaaS and includes the VMs, their OSs and platform applications. Some or all of these and those listed for IaaS are included in this Authorization Boundary if the CSP manages/secures the OS and platform applications.
          NOTE: Some PaaS services may not employ virtualization and the platform application offered by the service may be built from the ground up. This does not match the NIST definitions for cloud services.
        - SaaS: may build on the devices, platforms, applications, or constructs used in IaaS and PaaS to encompass the final application that constitutes the CSP's service offering and everything that supports it. Some or all of these and those listed for IaaS and PaaS are included in this Authorization Boundary for SaaS.
          NOTE: Some SaaS services may not employ virtualization and the application offered by the service may be built from the ground up. This does not match the NIST definitions for cloud services.

2. Mission Owner's system/application Authorization Boundary which is addressed by the Mission Owner's ATO. Mission Owner's system/applications inherit the C/CEs that the CSP implements for their organization and CSO(s) along with any resulting residual risk

based on how well the C/CEs are implemented. The Mission Owner's ATO covers these inherited C/CEs along with the following based on service type:

- IaaS: the Mission Owner operated/maintained system of virtual networks and VMs along with their OSs, applications, and associated data storage.
- PaaS: the portion of the system of virtual networks and VMs along with their OSs, platform applications, and associated data storage managed by the Mission Owner along with the application(s) implemented by the Mission Owner on top of the CSO.
- SaaS: The portion of the CSO managed by the Mission Owner (e.g., user accounts) along with the Mission Owner policies and procedures for using the CSO and the Mission Owner's compliance with DoD security policies related to the use of the CSO and Cloud in general.
- All service types: data in transit encryption methods used by the Mission Owner, any additional layers of access control implemented by the Mission Owner for access to the service for users and management, data at rest encryption implemented or managed by the customer, and any other DoD requirements that must be met by the CSP's customer.

4.3.2 Cloud Service Offering (CSO) Risk

The DoD PA provides a provisional or partial risk acceptance determination for the CSO against the appropriate DoD security requirements. The DoD PA assessment process assesses and highlights CSO risk based on its supported impact level. At level 4 and above, it's important to recognize that the DoD PA evaluation process also assesses the risk to DoD of permitting CSPs to connect to DoD networks.

4.3.3 Mission Risk

Mission refers to the information system and functions for which a DoD entity acquires or uses a CSO. This may be the direct use of a SaaS CSO in performing an IT-enabled mission, or the instantiation of an IT system or application on an IaaS/PaaS CSO.

Any DoD or Non-DoD CSO used by Mission Owners must have been issued a DoD PA by DISA. Overall mission risk will continue to be assessed and authorized by the Mission Owner's AO through the issuance of an ATO. The Mission Owner's system/application/cloud use case must be issued an ATO by their Component's AO or other component authorized subordinate AO directly responsible for risk acceptance for the Mission Owner's system/application/cloud use case. This is applicable at all information impact levels. This mission system ATO requirement extends to DoD CSP IaaS/PaaS CSOs where its ATO only permits its connection to the DISN since such an ATO cannot address full mission system/application risk when built on the CSO.

The requirement that a Mission Owner must only utilize CSOs that have a DoD PA extends to CSOs provided by a third party integration contractor or reseller of CSP CSOs. Any CSO being integrated into a solution for use by DoD or resold to a DoD entity must have a DoD PA.

Mission Owners categorize mission systems and/or applications in accordance with (IAW) DoDI 8510.01 defined processes. Mission owners then select CSOs from the DoD Cloud Service Catalog based on their security posture and the risk tolerance of the Mission Owner and their AO. While CSOs will have been assessed and provisionally authorized for use, the Mission

Owner must proceed IAW the RMF to obtain an Authority To Operate (ATO) from their assigned AO.

The Mission Owner inherits compliance from the CSO for the security controls (or portions thereof) that the CSP meets and maintains. A Mission Owner's system or application built on an IaaS or PaaS offering will be subject to meeting many of the same security controls within the system/application. Mission Owners contracting for SaaS offerings inherit the bulk of compliance with the security controls from the CSO. Inheritance will be different between CSPs operating within a given service model and thus must be evaluated separately. It should also be noted that the number of controls increases with higher impact levels and additional overlay controls (e.g. privacy). While Figure 2 depicts the division of management and ergo responsibility shared between the CSP and Mission Owner, it also illustrates the concept of inheritance.

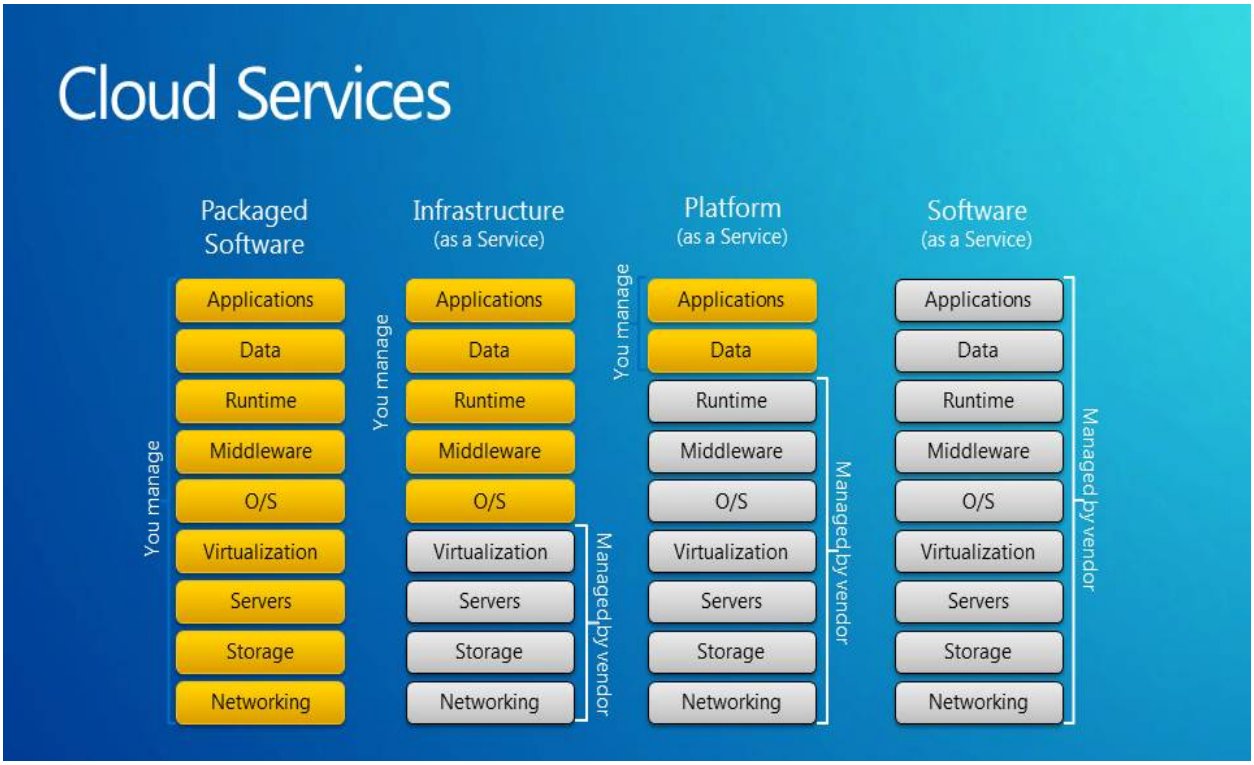

Figure 2 – Notional Division of Security Inheritance and Risk [36]

The benefit of starting with a provisionally authorized CSO is that much of the security controls assessment work is already accomplished. Mission Owners and their AOs must still review the FedRAMP and DoD PA artifacts to understand the risks that the mission will inherit when using the selected CSO for the mission system/application. Mission owners may need to implement, or request that the CSP implement, compensating controls for any risk deemed unacceptable prior to obtaining an ATO. Additional compensating controls must be reflected in the Mission Owner's SLA/contract with the CSP.

[36] Figure 2: Graphic courtesy of Microsoft

4.4 CSP Transition from CSM v2.1 to CC SRG v1r1 and Subsequent Updates

FedRAMP provides a transition strategy[37] for migrating CSP assessments from the FedRAMP v1 baselines based on NIST SP 800-53 rev3 to the FedRAMP v2 baselines based on NIST SP 800-53 rev4. This strategy went into effect on June 6, 2014. The key points are as follows:

- Any new assessment starting after June 1, 2014 will immediately transition to FedRAMP v2 baselines based on NIST SP 800-53 rev4.
- CSPs in the process of being assessed against FedRAMP v1 baselines based on NIST SP 800-53 rev3 prior to June 1, 2014 will continue on this track, but must transition to the FedRAMP v2 baselines within one year of their authorization date.
- CSPs currently in continuous monitoring will have until their next annual assessment to complete the transition to FedRAMP v2 baselines.

NOTE: In accordance with the original transition plan, FedRAMP updated its transition plan on 9 Sept, 2015[38] to state:

"FedRAMP requires all CSPs to transition to the FedRAMP Revision 4 requirements by the end of the 2015 calendar year. As of January 1, 2016, the FedRAMP PMO will not accept Revision 3 system documentation as FedRAMP compliant."

The requirements in this SRG become effective immediately upon final publication. However, the DoD migration plan for CSP assessments will mirror the FedRAMP plan as follows:

- Any new assessment starting after the release of this CC SRG will be assessed against these requirements.
- CSPs currently in the process of being assessed against the requirements in the CSMv2.1 will continue on this track, but must transition to compliance with the CC SRG requirements in coordination with their next FedRAMP/DoD annual assessment.
- CSPs currently in continuous monitoring under CSMv2.1 will have until their next FedRAMP/DoD annual assessment to complete the transition to compliance with the CC SRG control requirements.

A DoD PA issued for a CSP using the CSMv2.1 and based on FedRAMP v1 remains in effect for the duration of the DoD PA (unless revoked), so long as compliance is achieved within the timelines described above. DoD mission owner's systems leveraging a CSO may experience a period of time where risks based on FedRAMP v2 or new FedRAMP+ security controls have not yet been assessed. Mission owners and their AOs must review the controls to determine if the risk is acceptable until such time the CSP is required to comply or include the required compliance in the SLA/contract.

NOTE: CSPs wishing to transition sooner than later may do so at any time.

NOTICE: the use of the term FedRAMP v2 in the CC SRG refers to the FedRAMP baselines that were updated to NIST SP 800-53 rev4 from rev 3. This is not to be confused with the pending revision of FedRAMP designated as FedRAMP 2.0.

[37] FedRAMP transition strategy: www.fedramp.gov/files/2015/03/FedRAMP-Revision-4-Transition-Guide-v1.0-1.docx
https://www.fedramp.gov/files/2015/01/FedRAMP-Rev-4-Transition-Additional-Guidance.docx
[38] FedRAMP transition strategy 9/2015: https://www.fedramp.gov/files/2015/01/FedRAMP-Rev-4-Transition-Guide-v3-0.pdf

4.4.1 CSP Transition from CC SRG Version/Release to Updated CC SRG Version/Release

The requirements in CC SRG updates, whether they are a major version update or minor release update, become effective immediately upon final publication. However:

- Any new CSP/CSO assessment starting after the release of a CC SRG update will be assessed against the updated requirements.
- CSPs/CSOs currently in the process of being assessed against the requirements in the previous CC SRG will continue on this track, but must transition to compliance with the current CC SRG update in coordination with their next FedRAMP/DoD annual assessment. i.e., one year from award of the PA.
- CSPs/CSOs currently in continuous monitoring under the previous CC SRG will provide a Plan of Action and Milestones (POA&M) within 30 days for becoming compliant with the current CC SRG requirements as soon as possible, but no later than, their next FedRAMP/DoD annual assessment if scheduled six months after the CC SRG update is released, not to exceed one year. i.e., transition is to occur as soon as practical but no longer than between six months and one year.

A DoD PA issued for a CSP using the previous CC SRG and based on FedRAMP v2 remains in effect for the duration of the DoD PA (unless revoked), so long as compliance is achieved with the timelines described above. Due to the transition period, DoD mission systems leveraging a CSO may experience a period of time where risks based on the current CC SRG security controls have not yet been assessed. Mission owners and their AOs must review the controls to determine if the risk is acceptable until such time the CSP is required to comply or include the required compliance in the SLA/contract.

NOTE: CSPs wishing to transition sooner than later may do so at any time.

4.5 DoD PA in Relation to RFP Response and Contract Award

This section provides information relative to provisional authorizations and contract awards. The following points, in no way, alter any contract clauses currently defined in the Defense Federal Acquisition Regulation Supplement (DFARS) or may be defined in the future.

While it is always desirable for a CSP to have a DoD PA before responding to a DoD cloud services RFP, DoD is not making this as a precondition or prequalification to a response or award of a contract. However, a DoD PA and a Mission Owner ATO is required to be in place before the contracted service goes into production with live DoD data.

Each CSP responding to an RFP that does not already have a DoD PA at the required information impact level will submit all required FedRAMP and DoD documentation relevant to being assessed for a DoD PA with the RFP response. This is so that the documentation package can be initially reviewed for completeness and the likelihood that the FedRAMP and FedRAMP+ requirements are or can be met toward award of the required DoD PA. The DISA SCA organization, at the request of the contracting officer or Mission Owner's AO, will make a quick-look review of the assessment package from the apparently successful offeror and report the results back. If the process moves forward, DISA will work with the CSP toward meeting the requirements and subsequent award of the DoD PA for the CSO as is done for any PA assessment. If the apparently successful offeror does not provide the required assessment

documentation or cannot meet the security requirements for receiving a DoD PA based on an acceptable level of risk, the offeror may be disqualified by the contracting officer.

This extends to integrators and resellers of CSP CSOs responding to RFPs. Any CSO being integrated into a solution for use by DoD or resold to a DoD entity must have a DoD PA.

This page is intentionally blank.

5 SECURITY REQUIREMENTS

This section of the CC SRG defines the security requirements for DoD's use of cloud computing. It covers several areas as follows:

- Security requirements for assessing CSOs for the award of a DoD PA and inclusion in the DoD Cloud Service Catalog.
- Security requirements for CSP's/CSOs while hosting DoD missions.
- Security requirements for Mission Owner's systems/applications using or built on CSOs.

NOTICE: All CSP and CSO requirements in this CC SRG apply to all CSPs and CSOs offered to or contracted by the DoD. DoD recognizes that CSOs may be offered by a CSP or an Integrator as the prime contractor on a DoD contract. DoD also recognizes that prime contractors may subcontract for multiple CSOs to meet contract capabilities requirements and may subcontract systems maintenance. Therefore all requirements in this CC SRG apply to all CSOs provided by prime contractors and their subcontractors to include systems maintenance contractors who may have access to CSP customer information or who may have the capability of affecting the security of the CSO. This flow down to subcontractors is also covered in cloud and contractor associated DFARS clauses.

5.1 DoD Policy Regarding Security Controls

DoDI 8500.01 requires all DoD Information Systems to be categorized in accordance with CNSSI 1253 and implement a corresponding set of security controls and control enhancements (C/CEs) that are published in NIST SP 800-53, regardless of whether they are National Security Systems (NSS) or non-NSS.

The CNSSI 1253 baselines are tailored from the NIST SP 800-53 recommended baselines, as are the FedRAMP baselines. These baselines are a starting point for securing all DoD systems, which can be tailored further to address specific systems and situations.

See NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*,[39] for a definition of NSS and further information.

5.1.1 DoD use of FedRAMP Security Controls

The FedRAMP Low and Moderate baselines are a tailored set of C/CEs based on the Low and Moderate baselines recommended in NIST SP 800-53 catalog of security controls.

The 15 December 2014 DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services* states "FedRAMP will serve as the minimum security baseline for all DoD cloud services." This SRG uses the FedRAMP v2 Moderate baseline at all information impact levels.

The 2014 DoD CIO memo further states "components may host Unclassified DoD information that has been publicly released on FedRAMP approved cloud services". Using the definitions defined in Section 3.2, Impact Level 2 information may be hosted in a CSP that minimally holds a FedRAMP Moderate PA (with or without a DoD PA); subject to compliance with the

[39] NIST SP 800-59: http://csrc.nist.gov/publications/PubsSPs.html

personnel security requirements outlined in Section 5.6.2, *CSP Personnel Requirements* and acceptance by the Mission Owner and the responsible AO. The FedRAMP v2 Moderate baseline, supplemented with DoD FedRAMP+ C/CEs and requirements in this SRG, are used to assess CSPs toward awarding a DoD PA at information impact levels 4 and above. Only FedRAMP v2 Moderate baseline controls will be assessed for DoD PAs for impact level 2. This in no way alleviates the CSP from meeting the security requirements for CSP's/CSOs while hosting DoD IT missions or the Mission Owner from securing their systems/web sites/applications in Level 2 CSOs.

5.1.2 DoD FedRAMP+ Security Controls/Enhancements

DoD FedRAMP+ refers to a tailored baseline of security C/CEs which has been developed for each DoD information impact level, except for level 2. These baselines incorporate, but are not limited to, the FedRAMP Moderate baseline. The FedRAMP+ C/CEs include NIST 800-53 security controls and enhancements not included in the FedRAMP Moderate baseline. FedRAMP+ also includes tailored values and selections for most FedRAMP and FedRAMP+ C/CEs which require definition. The FedRAMP+ C/CEs were selected primarily because they address issues such as the Advanced Persistent Threat (APT) and/or Insider Threat, and because the DoD, unlike the rest of the Federal Government, must categorize its systems in accordance with CNSSI 1253, use its baselines, and then tailor as needed.

The CNSSI 1253 baseline used in support of DoD PAs is based on Moderate Confidentiality and Moderate Integrity. It does not include a baseline for Availability (categorization designated as M-M-x). Availability is addressed in the FedRAMP baseline and may also be addressed by the Mission Owner in the contract/SLA. The resulting M-M-x baseline was compared to the FedRAMP Moderate baseline to derive a tailored set of FedRAMP+ security controls/enhancements for each level. This comparison indicated that the FedRAMP Moderate Baseline includes approximately thirty two (32) C/CEs that are also contained in the CNSSI 1253 M-M-x baseline, but not in the NIST 800-53 Moderate baseline incorporated in both. The comparison also indicated that eighty-eight (88) of the C/CEs in the CNSSI 1253 M-M-x baseline are not in the FedRAMP Moderate baseline. These 88 were analyzed for their security benefit in the CSP environment and projected cost if the CSP were required to implement the C/CE. Approximately half were selected for the DoD cloud baselines for assessing CSPs. The number of control enhancements selected varies by impact level.

Table 2 provides a listing of the FedRAMP+ C/CEs applicable to each information impact level, which includes only one additional base control. The rest are control enhancements. This table does not include controls added by the Classified Information or Privacy overlays. More information on the assessment of the C/CE in these overlays is provided in the sections following this one.

NOTE: This table does not include the FedRAMP Moderate baseline C/CEs, a table of which can be obtained from the FedRAMP website on the Documents page[40].

Table 2 - DoD FedRAMP+ Security Controls/Enhancements

[40] FedRAMP website: www.fedramp.gov/resources/documents

SP 800-53r4 Cont./Enh. ID	Level 4	Level 5	Level 6
AC-06 (07)	X	X	X
AC-06 (08)	X	X	X
AC-17 (06)	X	X	X
AC-18 (03)	X	X	X
AC-23	X	X	X
AT-03 (02)	X	X	X
AT-03 (04)	X	X	X
AU-04 (01)	X	X	X
AU-06 (04)	X	X	X
AU-06 (10)	X	X	X
AU-12 (01)	X	X	X
CA-03 (01)		X	n/a*
CM-03 (04)	X	X	X
CM-03 (06)	X	X	X
CM-04 (01)	X	X	X
CM-05 (06)	X	X	X
IA-02 (09)	X	X	X
IA-05 (13)	X	X	X
IR-04 (03)	X	X	X
IR-04 (04)	X	X	X
IR-04 (06)	X	X	X
IR-04 (07)	X	X	X
IR-04 (08)	X	X	X
IR-05 (01)	X	X	X
IR-06 (02)	X	X	X
MA-04 (03)	X	X	X

MA-04 (06)	X	X	X
PE-03 (01)	X	X	X
PL-08 (01)		X	X
PS-04 (01)		X	X
PS-06 (03)		X	X
SA-04 (07)		X	X
SA-12	X	X	X
SA-19	X	X	X
SC-07 (10)	X	X	X
SC-07 (11)		X	X
SC-07 (14)			X
SC-08 (02)		X	X
SC-23 (01)	X	X	X
SC-23 (03)	X	X	X
SC-23 (05)		X	X
SI-02 (06)	X	X	X
SI-03 (10)		X	X
SI-04 (12)	X	X	X
SI-04 (19)	X	X	X
SI-04 (20)	X	X	X
SI-04 (22)	X	X	X
SI-10 (03)	X	X	X
Total	38 Also see 5.1.5	47 Also see 5.1.4 5.1.5	47 Also see 5.1.4 5.1.4.1

* Most Level 5 FedRAMP+ C/CEs are also applicable at Level 6. The use of n/a in Level 6 for CA-03 (01) is because the CE addresses "Unclassified National Security System Connections" and is therefore not selectable or applicable for Classified NSS.

NOTE: CSPs may offer equivalent controls or mitigations which will be considered on a case-by-case basis.

5.1.3 Parameter Values for Security Controls and Enhancements

Both FedRAMP and the DoD have defined minimum requirements in security controls and enhancement parameters. However, in some circumstances, the specifics of the implementation are left to the CSP and assessed as to whether the implementation is appropriate for the CSO and government. For those controls required by FedRAMP and the DoD, the parameter values are defined in Appendix D - *CSP Assessment Parameter Values for PA.* Also see Section 5.1.5.2, *Effects of the Privacy Overlay on CSPs and Mission Owners* for additional parameter guidance.

5.1.4 National Security Systems (NSS)

Although the control baselines for all levels are based on those from CNSSI 1253, only impact Level 5 and 6 are designed to accommodate NSS categorized up to M-M-x. NSS-specific C/CEs have been included at these levels along with those required for the slightly higher impact of these systems at the moderate level (short of a full high baseline). Thus, unclassified NSS must be instantiated at level 5 if a CSO is used. This, however, does not preclude an unclassified non-NSS from operating at Level 5 if the mission/information owner requires the added security.

5.1.4.1 NSS Level 6 Classified Overlay Applicability

Impact Level 6 is for classified systems which by definition are NSS. As such and IAW the DoD RMF, **on-premises** CSOs are subject to the CNSSI 1253 Classified Information Overlay in addition to FedRAMP and FedRAMP+. This overlay is an attachment to Appendix F of the CNSSI 1253 entitled *CNSSI 1253F, Attachment 5, Classified Information Overlay*.[41] It is available from the CNSS Library on the Instructions page.

This overlay imposes 94 additional C/CEs which must be assessed for a CSP's CSO Level 6 PA. For all CSOs, there may only be a portion of these C/CEs applicable to the CSP with the balance of the C/CEs being fulfilled by the Mission Owner. This division of responsibility will be addressed in a future release of this document or in a companion document.

5.1.5 CNSSI 1253 Privacy Overlay

The CNSSI 1253 Privacy Overlay is an attachment to Appendix F of the CNSSI 1253 entitled *CNSSI 1253F, Attachment 6, Privacy Overlay*.[42] It is available from the CNSS Library on the Instructions page.

The Privacy Overlay was developed in accordance with Federal privacy requirements found in laws, policies, and standards that apply to government agencies, such as the *Privacy Act of 1974* [43]and *HIPAA*[44], leveraging experts and lawyers in both fields. Legal references are included as the basis for all control specifications in the Privacy Overlay, including whether to

[41] Classified Information Overlay: https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[42] Privacy Overlay: https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[43] Privacy Act: http://www.archives.gov/about/laws/privacy-act-1974.html
[44] HIPAA: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html

select or exclude C/CE as well as the provision of supplemental guidance and control extensions. It is supported by DoD and the IC as well as other Federal agencies that are part of the CNSS. The Privacy Overlay was written by CNSS to protect PII and PHI in NSS, however, many of the requirements the overlay specifications are based on apply to any Federal information system that contains PII or PHI, regardless of whether the system is an NSS or not. All Federal agencies including DoD must comply with public laws that apply to the Federal government's collection, use and maintenance of PII, thus DoD invokes the CNSS Privacy Overlay since it is the best resource we know of.

This overlay addresses Low, Moderate, and High sensitivity PII and PHI. It invokes most of the 36 privacy specific C/CEs from NIST SP 800-53 rev4, *Appendix J, Privacy Control Catalog* and invokes additional C/CEs from the *Security Control Catalog*. It also modifies many of the already selected C/CEs in the FedRAMP Moderate and FedRAMP+ baselines by providing supplemental guidance along with parameter value changes and control extensions. Quantities of additional C/CEs and guidance depend on both the PII sensitivity level and whether the PII meets the definition of PHI.

5.1.5.1 PII/PHI at Level 2

PII and PHI are categorized as CUI and as such must minimally be stored and processed in a Level 4 CSO. While the Privacy Overlay provides a Business Rolodex Exception (BRE) which exempts a subset of low sensitivity PII from the protection of the overlay, this does not remove this PII from the CUI category. Therefore at this time, no PII/PHI is permitted to be processed or stored in Level 2 CSOs.

5.1.5.2 Effects of the Privacy Overlay on CSPs and Mission Owners

To limit the affect the listing of Privacy Overlay C/CE and their Parameter Values on the size of the main portion of the CC SRG, this section provides pointers to tables in Appendix E of Privacy Overlay C/CE in the following categories:

- FedRAMP Moderate and FedRAMP+ C/CE that are modified through Control Extensions or altered via implementation guidance or value specifications. These tables also include C/CE that are required by law or regulation:
    - Table 10 - FedRAMP M C/CE Modified or Required by Regulation
    - Table 11- FedRAMP+ C/CE Modified or Required by Regulation
- C/CE not included in the DoD cloud baseline which includes FedRAMP Moderate and FedRAMP+ C/CE. This includes some C/CE designated as SLA C/CE as shown in Section 5.1.6, *Security Controls/Enhancements to be optionally addressed in the Contract/SLA* and some CNSSI 1253 C/CE that were not selected for inclusion in the FedRAMP+ or SLA C/CE sets:
    - Table 12 - *Privacy Overlay C/CE Not Included In FedRAMP M* or FedRAMP+
- C/CE that are in the FedRAMP Moderate and FedRAMP+ C/CE baselines that have parameter values defined by the overlay which may modify the parameter values defined in Table 8 – *FedRAMP M / FedRMP+ Control / Enhancement Parameter* Values for PA Assessment:
    - Table 13 - *PII/PHI Parameter Values for FedRAMP and FedRAMP+ C/CE*
- C/CE not included in the DoD cloud baseline which includes FedRAMP Moderate and FedRAMP+ C/CE that have parameter values defined by the overlay.

- Table 14 - *PII/PHI Parameter Values for C/CE Not Included In FedRAMP M or FedRAMP+*

NOTE: a comparative analysis of the Privacy Overlay C/CE to various other baselines is provided in Appendix F. This comparison provides statistics or counts of C/CE in various categories. This is provided for informational purposes only and may be removed from the final document or a future release of the CC SRG.

5.1.5.3 CSO Assessment of Privacy Overlay Control/Control Enhancements

CSP CSOs that are intended to store and process PII and/or PHI (e.g., certain SaaS and PaaS offerings and potentially others) must be additionally assessed against the C/CEs that the Privacy Overlay adds to, or modifies in, the FedRAMP Moderate baseline as well as the FedRAMP+ C/CEs to receive a DoD PA for the CSO. This includes all SLA C/CEs and the Deselected C/CE from the CNSSI 1253 M-M-x baseline (used to select the FedRAMP+ C/CEs) that show a + symbol in the overlay which are to be added to the FedRAMP+ table at the appropriate level.

Successful Privacy Overlay assessments will result in a rider or qualifier to the DoD PA that will reference the level of PII or PHI the CSO was successfully assessed for. E.g., CSO xyz is granted a Level 4 PA with the additional provisional authorization to handle up to Moderate sensitivity PII, or to handle some level of PII and PHI. Privacy Overlay C/CE that are clearly the responsibility of the CSP's customer i.e., DoD Mission / Information Owner (e.g., the required Systems of Record Notice (SORN) per TR-2), will not be assessed and will not affect the award of a DoD PA.

It is also recognized that while IaaS and some PaaS CSOs have the potential to store and process PII and/or PHI, this is mostly at the customer's discretion, and is not typically the intent of the CSP. As such, Privacy Overlay assessment will not be required for the IaaS and some PaaS CSO to receive a DoD PA.

Additionally, while a CSP's IaaS and some PaaS CSOs will not normally be assessed against the Privacy Overlay, it is recognized that there may be some C/CE that may become the responsibility of the CSP if the Mission Owner chooses to store and process PII and/or PHI in the CSO. Typically, assessment of these C/CEs would be negotiated by the Mission Owner with the CSP. There is also the potential that a CSP might want a DoD PA rider so that their IaaS/PaaS CSO could be pre-approved to handle such missions.

NOTE: Some PaaS CSOs are intended to handle PII/PHI like some SaaS CSOs. These are typically very much like a SaaS CSO and as such must be assessed against the Privacy Overlay.

NOTE: more specific guidance regarding what Privacy overlay C/CEs apply to CSPs vs Mission Owners will be provided in a future release of this SRG.

5.1.5.4 Mission System / Application Assessment of Privacy Overlay Control/Control Enhancements

If the Mission Owner's cloud system/application is intended to store and process PII and/or PHI, the system/application must already comply with the privacy requirements which are codified in the Privacy Overlay. Therefore, Privacy Overlay assessment to include PA riders must be incorporated into a Mission Owner's CSP evaluation /selection/acquisition process and into their assessment process for their mission system's ATO.

NOTE: more specific guidance regarding what Privacy overlay C/CEs apply to CSPs vs Mission Owners will be provided in a future release of this SRG.

5.1.6 Security Controls/Enhancements to be optionally addressed in the Contract/SLA

Table 3 shows the C/CEs designated for the Mission Owner to optionally address in the contract or SLA, over and above the FedRAMP and FedRAMP+ C/CEs which must be included by default. While these C/CEs generally address system availability, they apply to the availability of information related to continuous monitoring, incident response, and other security issues. It must be noted that 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 rev4 in the contract/SLA if they need the control/enhancement to be provided/met by the CSP to secure their system or application. Assessment and continuous monitoring of compliance with these C/CEs is the responsibility of the Mission Owner as negotiated with the CSP in attaining and maintaining the mission's ATO. These C/CEs are not assessed toward the award of a DoD PA at this time.

Table 3 - Security Controls/Enhancements 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
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		
PS-06 (03)	X		
SC-07 (11)	X		
SC-07 (14)	X	X	
SC-18 (03)		X	X
SC-18 (04)		X	X
Total	9	10	9

5.2 Legal Considerations

This section deals with legal requirements revolving around the location of DoD information as well as who may have access to it in CSP facilities and CSOs.

5.2.1 Jurisdiction/Location Requirements

Legal jurisdiction over information controls where DoD and US government data can be located. This is nuanced by the information being on DoD Premises.

Corresponding Security Controls: SA-9(5)

5.2.1.1 Jurisdiction/Location Requirements for DoD Off-Premises Locations

To protect against seizure and improper use by non-US persons and government entities, all data stored and processed by/for the DoD must reside in a facility under the exclusive legal jurisdiction of the US. CSPs will maintain all government data that is not physically located on DoD premises within the 50 States, the District of Columbia, and outlying areas of the US (as defined at FAR 2.101[45]), unless otherwise authorized by the responsible AO, as described in DoDI 8510.01. The contracting officer shall provide written notification to the contractor when the contractor is permitted to maintain Government data at a location outside the 50 States, the District of Columbia, and outlying areas of the United States.

CSPs will provide the agency a list of the physical locations where the data could be stored at any given time and update that list as new physical locations are added.

5.2.1.2 Jurisdiction/Location Requirements for DoD On-Premises Locations

DoD on-premises includes DoD data centers, other facilities located on a DoD 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. A commercial facility, in this sense, means a building or space leased and controlled by DoD. Physical facilities may be permanent buildings or portable structures such as transit/shipping containers. An example of the latter might be a container housing a commercial CSP's infrastructure located adjacent to a Core Data Center (CDC) and connected to its network as if it was inside the building.

DoD CSPs will, and commercial CSPs may (under DoD contract), instantiate their cloud service architecture on DoD premises (DoD on-premises). Interconnection with DoD networks will be interoperable IAW engineering requirements that meet cybersecurity guidance and controls. Such implementations will be considered DoD Private.

On-premises CSOs implemented by a DoD or non-DoD CSP which utilizes a hybrid model employing off-premises CSPs and CSOs to augment the on-premises CSO must meet the location requirements stated in Section 5.2.1.1, *Jurisdiction/Location Requirements* for DoD Off-Premises Locations.

[45] FAR 2.101: http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/02.htm

5.2.2 Cloud Deployment Model Considerations / Separation Requirements

The risks and legal considerations in using virtualization technologies further restrict the types of tenants that can obtain cloud services from a virtualized environment on the same physical infrastructure and the types of cloud deployment models (i.e., public, private, community, and hybrid) in which the various types of DoD information may be processed or stored.

While shared cloud environments provide significant opportunities for DoD entities, they also present unique risks to DoD data and systems that must be addressed. These risks include exploitation of vulnerabilities in virtualization technologies, interfaces to external systems, APIs, and management systems. These have the potential for providing back door connections and CSP privileged user access to customer's systems and data. While proper configuration of the virtual and physical environment can mitigate many of these threats, there is still residual risk that may or may not be acceptable to DoD. Legal concerns such as e-discovery and law enforcement seizure of non-government CSP customer/tenant's data pose a threat to DoD data if it is in the same storage media. Due to these concerns, DoD is currently taking a cautious approach with regard to Level 5 information.

Infrastructure (as related to cloud services), is the physical hardware (i.e., servers and storage), and the network interconnecting the hardware that supports the cloud service and its virtualization technology (if used). This includes the systems and networks used by the CSP to manage the infrastructure. While the physical space in which this infrastructure is housed is part of the CSP's infrastructure, this is not a factor in DoD's separation restrictions except at Level 6.

Dedicated infrastructure (as related to cloud services) refers to the cloud service infrastructure being dedicated to serving a single customer organization or a specific group of customer organizations. A private cloud service implements dedicated infrastructure to serve one customer organization. This SRG considers DoD as the organization which consists of all DoD components. This SRG restricts private cloud for DoD as meaning dedicated infrastructure that serves DoD users and tenants, and designates this as a DoD private cloud. DoD private clouds or cloud service offerings may be multi-tenant serving all or some DoD components or may be single tenant serving a single mission. A community cloud service implements dedicated infrastructure to serve a specific group or class of customer organizations. Since the definition of DoD private could also be considered a DoD community cloud, this SRG will use the term DoD private/community. This SRG will also use the term Federal Government community, meaning dedicated multi-tenant infrastructure that serves both DoD components and mission owners as well as other Federal Government agencies and their mission owners.

Corresponding Security Controls: SC-4

5.2.2.1 Impact Level 2 Location and Separation Requirements

Impact Level 2 cloud services can be offered on any of the four deployment models. Information that may be processed and stored at Impact Levels 2 can be processed on-premises or off-premises, as long as the physical location of the information is restricted as described in Section 5.2.1, *Jurisdiction/Location Requirements*.

For a Level 2 PA, at this time, DoD is accepting the risk that this is adequately covered by a FedRAMP Moderate PA such that the requirement will not be additionally assessed for a Level 2 PA.

5.2.2.2 Impact Level 4 Location and Separation Requirements

Impact Level 4 cloud services can be offered on any of the four deployment models. Information that may be processed and stored at Impact 4 can be processed on-premises or off-premises, as long as the physical location of the information is restricted as described in Section 5.2.1, *Jurisdiction/Location Requirements*.

For a Level 4 PA, the CSP must provide evidence of strong virtual separation controls and monitoring in support of the ability to meet "search and seizure" requests for non-DoD information and data without the release of DoD information and data and vice-versa. Additionally the strong virtual separation controls must prevent/mitigate/eliminate the potential vulnerability whereby one CSP customer using the same physical hardware as another CSP customer can gain access to the other's information/data, virtual network, or virtual machines. Monitoring must detect such unauthorized accesses and/or attempts so that incident response can occur.

5.2.2.3 Impact Level 5 Location and Separation Requirements

Information that must be processed and stored at Impact Level 5 can only be processed in a DoD private/community or federal government community cloud, on-premises or off-premises in any cloud deployment model that restricts the physical location of the information as described in Section 5.2.1, *Jurisdiction/Location Requirements.*

The following also applies:

- Only DoD private/community or Federal Government community clouds are eligible for Impact Level 5.
- Each deployment model may support multiple missions or tenants / missions from each customer organization.
- Virtual/logical separation between DoD and Federal Government tenants / missions is sufficient. Virtual/logical separation between tenant/mission systems is minimally required.
- Physical separation from non-DoD/non-Federal Government tenants (i.e., public, local/state government tenants) is required.
- The CSP restricts potential access to DoD's and the community's information to CSP employees that are U.S. Citizens

NOTE: While multi-tenant CSOs marketed as ITAR compliant", "government clouds", or "clouds for government" might restrict data location to US jurisdiction, and might restrict the personnel that manage the CSO to , they do not necessarily meet the standard for "dedicated" to the Federal Government or DoD. If the cloud service, or the underlying infrastructure it resides on, hosts any non-Federal US government tenant, (such as state, local, or tribal governments, industry/academic partners, or foreign governments) it is considered a public cloud for purposes of this SRG. As such, while DoD sees this as adequate for Level 4, this alleged attribute is not sufficient for CSP selection by DoD Mission Owners for Level 5 missions. This restriction might be waived by DoD if the CSP and CSO can demonstrate sufficient separation between tenant's workloads and data and/or the general government community and Federal Government Community.

5.2.2.4 Impact Level 6 Location and Separation Requirements

Impact Level 6 is reserved for the storage and processing of information classified up to SECRET. Information that must be processed and stored at Impact Level 6 can only be processed in a DoD private/community or Federal Government community cloud, on-premises or off-premises in any cloud deployment model that restricts the physical location of the information as described in Section 5.2.1, *Jurisdiction/Location Requirements.*

The following applies:

- Impact Level 6 information up to the SECRET level must be stored and processed in a dedicated cloud infrastructure located in facilities approved for the processing of classified information, rated at or above the highest level of classification of the information being stored and/or processed.
- Impact Level 6 CSO infrastructure is considered to be a SIPRNet enclave and as such will be a closed self-contained environment for the CSO processing, storage, and management planes only connected to SIPRNet.
- Each deployment model may support multiple SECRET missions from multiple customer organizations.
- Virtual/logical separation between DoD and Federal Government tenants / SECRET missions is sufficient.
- Virtual/logical separation between tenant/mission systems is minimally required.
- Physical separation from non-DoD/non-Federal Government tenants (i.e., public, local/state government tenants) is required.

5.2.2.5 Separation in Support of Law Enforcement and Criminal Investigation and E-Discovery

Under Federal law, the Federal government reserves the right for law enforcement officials to perform criminal investigations of Federal Government employees and elected officials as well as anyone with access to Federal Government information for misconduct, misuse of such data, or for incident investigation. Such criminal investigations may include a need for E-Discovery on Federal government information to collect digital evidence. As such the CSP must be able to segregate Federal government information from non-Federal Government information within the CSO. The granularity of separation must be at the Federal government Mission Owner level. The CSP must also ensure this segregation requirement flows down to all CSP/Integrator subcontracted CSP/CSOs. The CSP and subcontractors must then be capable, upon request of the contracting officer(s) or in response to a subpoena, of isolating one or more Federal Government Mission Owner's data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space or via secure remote connection with access limited to authorized Government personnel identified by the Contracting Officer, and without the CSP's involvement or provide a forensic digital image of the requested Federal government information. See Section 6.4.4, *Digital Forensics in the Cloud and Support for Law Enforcement/Criminal Investigation* for additional information on capturing and protecting forensic digital images.

5.2.3 DoD Data Ownership and CSP Use of DoD Data

All DoD information/data placed or created by DoD users in a CSP's CSO is owned by the DoD, the Mission Owner, and/or their Information Owner unless otherwise stipulated in the CSP's contract with the DoD. The CSP has no rights to the DoD's information/data. DoD information/data includes logs and monitoring data created within and by a Mission Owner's system/application implemented in IaaS/PaaS CSOs as well as logs created for and provided to the Mission Owner related to their usage and management of the CSO. DoD also maintains ownership of all information/data created by the CSP/CSO for DoD if such activities are part of the contract. CSPs seeking a DoD PA must agree that DoD remains the owner of all DoD data in a CSO.

CSPs are prohibited from using DoD data in any way other than that required to provide contracted services to DoD (e.g., customer access/usage logs used for billing) This means that the CSP may not "data mine" DoD email, files, information in data bases, or communications for any purpose other than that stipulated in the contract.

The CSP maintains ownership of all logs and monitoring data created within the CSO related to the Mission Owner's usage and management of the CSO. This includes logs related to customer access and usage used for billing, data used for capacity planning for the CSO, monitoring data related to malicious activities or CSO health. This also includes all audit content specified by the AU-2 security control for the time period specified by AU-11. While the CSP retains ownership of this information, some or all must be shared with the Mission Owner for the purpose of planning, forensics, billing validation, retention, etc. The ownership of the copies of this information shared with the DoD/Mission Owner is maintained by the DoD/Mission Owner.

Additionally, all DoD information/data and CSP information/data shared with the Mission Owner must be made available for off-boarding and backup IAW sections 5.8, *Data Retrieval and Destruction for Off-boarding from a CSO* and 5.12 - *Backup*.

Mission Owners must address data ownership in the contract.

Related Security Controls: AC-23

5.3 Ongoing Assessment

Both FedRAMP and DoD require an ongoing assessment and authorization capability for CSOs providing services to the DoD. This capability is built upon the DoD RMF and the FedRAMP continuous monitoring strategy, as described in the *Guide to Understanding FedRAMP* [46]and *FedRAMP Continuous Monitoring Strategy Guide.*[47] These ongoing assessment processes which are discussed in the following sections include continuous monitoring and change control.

Ongoing assessment processes do not differ by impact level, though the artifacts produced as part of those processes may. (e.g., Level 2 CSOs will have fewer controls to monitor than Level 4 CSOs.) These processes will differ, however, based on whether or not CSOs are part of the FedRAMP catalog or have a FedRAMP JAB PA. These differences are based on the division of

[46] Guide to Understanding FedRAMP: https://www.fedramp.gov/resources/documents/
[47] FedRAMP Continuous Monitoring Strategy Guide: https://www.fedramp.gov/resources/documents/

responsibility over the set of security controls and the ability of DoD to access the artifacts produced as part of the FedRAMP processes.

Ongoing assessment responsibility mirrors the divided responsibilities and control inherent in cloud systems. FedRAMP's processes will be leveraged for all CSOs in the FedRAMP catalog. This process, however, only covers the portion of the system that is governed by the FedRAMP PA, such as the FedRAMP Moderate security controls. The DoD change control process will cover the portion of the system that is governed by the DoD PA, such as the FedRAMP+ security controls. Ongoing assessment of controls that are levied by the Mission Owner, such as those specified in the SLA, and do not fall under the FedRAMP or DoD PAs is the responsibility of the Mission Owner. This division of responsibility is shown in Figure 3.

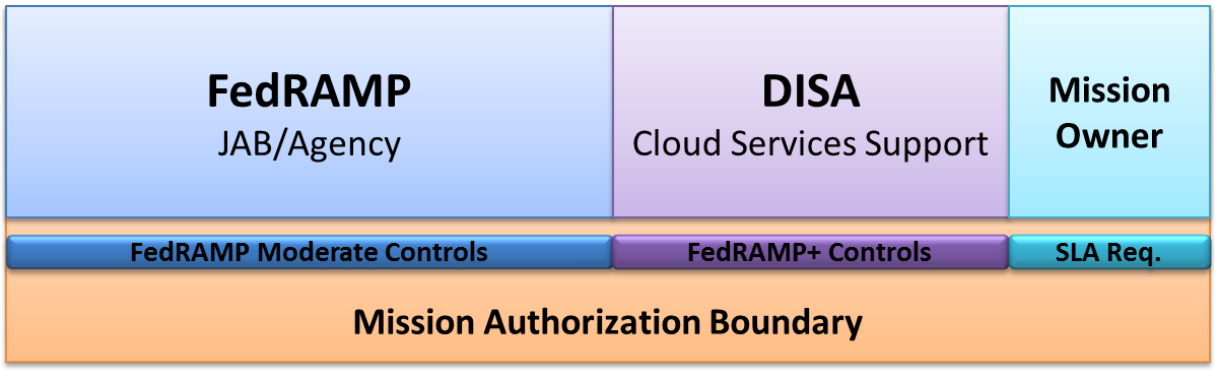

Figure 3 - Ongoing Assessment Division of Responsibility

5.3.1 Continuous Monitoring

This section pertains specifically to continuous monitoring of security controls, as defined by CNSSI 4009 and NIST SP 800-137. Further information on monitoring activities performed as part of Computer Network Defense, are described in Section 6, *Cyber Defense and Incident Response.*

Once a DoD PA is granted, the CSP is expected to maintain the security posture of the CSO through continuous and periodic vulnerability scans, DoD annual assessments, incident management, and effective implementation of operational processes and procedures. Integral to this is periodic reporting to the appropriate AO. The continuous monitoring artifacts required to maintain a DoD PA are the same as those required by FedRAMP. (Annual assessments, monthly vulnerability scans, etc.) However, those artifacts must include additional information for FedRAMP+ controls and DoD requirements.

Continuous monitoring data flows will differ for CSPs depending on whether their CSOs have a FedRAMP JAB PA, a 3PAO assessed non-DoD Federal Agency ATO, or DoD Assessed PA (as described in Section 4). These data flows are reflected in Figure 4, Figure 5, and Figure 6 respectively.

In some cases, CSPs such as, but not limited to, DoD Private CSOs or CSOs in the FedRAMP catalog with a non-DoD Agency ATO will provide continuous monitoring artifacts directly to DISA. In such cases, the CSP will utilize commercial standard formats (e.g., comma-separated values, XML) that enable DoD to automate the ingest of continuous monitoring data.

NOTE: For XML exchanges, National Information Exchange Model (NIEM) based XML is the preferred format IAW DoDI 8320.07[48], August 3, 2015. Additional information regarding this format can be found at www.niem.gov.

All CSP CSOs are required to have FedRAMP annual assessments performed by a 3PAO for the maintenance of their FedRAMP PA. DoD also requires annual assessments performed by a 3PAO or approved DoD SCA organization for the maintenance of their Level 4 and above DoD PA. It is expected that CSOs in both the FedRAMP and DoD catalogs will have a single annual assessment to cover this requirement for both FedRAMP and DoD. CSOs in the FedRAMP catalog will follow the process described in the *FedRAMP Continuous Monitoring Strategy Guide*[49]. DoD Annual assessments will minimally include the set of controls listed in Appendix A of that document, as well as any other controls specified by the DISA AO. CSOs with a DoD PA that are not in the FedRAMP catalog will follow the DoD RMF process for continuous monitoring and associated assessments.

Corresponding Security Controls: CA-7

5.3.1.1 CSOs in the FedRAMP Catalog

As described in Section 4.1, *Assessment of Commercial/Non-DoD Cloud Services*, the CSOs in the FedRAMP catalog that are eligible for DoD PAs include CSOs having a JAB PA (which is 3PAO assessed) or a 3PAO assessed Federal Agency ATO. All reports required by the *FedRAMP Continuous Monitoring Strategy Guide*, including self- assessments, for these CSOs will be provided to the FedRAMP Information System Security Officer (ISSO). These will be reviewed by the FedRAMP TRs (which include DoD personnel) and approved by the JAB if necessary.

Continuous monitoring requirements for DoD are the same as those for FedRAMP, except that all reports and artifacts for FedRAMP+ C/CEs will be provided directly to DISA AO representatives as the DoD single point of CSP contact for this information. DISA will share appropriate continuous monitoring information (FedRAMP and FedRAMP+) with Mission Owners, AOs, and Cyber Defense Service Providers (CDSPs).

The information will be used by Mission Owners, their AOs, and the DISA AO to assess and authorize the CSO. Those evaluations will inform decisions to continue the ATO for the Mission Owner's system and the PA for the CSP respectively. The DISA AO will coordinate closely with Mission Owners in the event that the withdrawal of a PA must be considered upon the basis of this requirement.

Figure 4 shows the normal flow of continuous monitoring information if the CSP has a FedRAMP JAB PA.

[48] DoDI 8320.07: http://www.dtic.mil/whs/directives/corres/pdf/832007p.pdf
[49] FedRAMP Continuous Monitoring Strategy Guide: https://www.fedramp.gov/resources/documents/

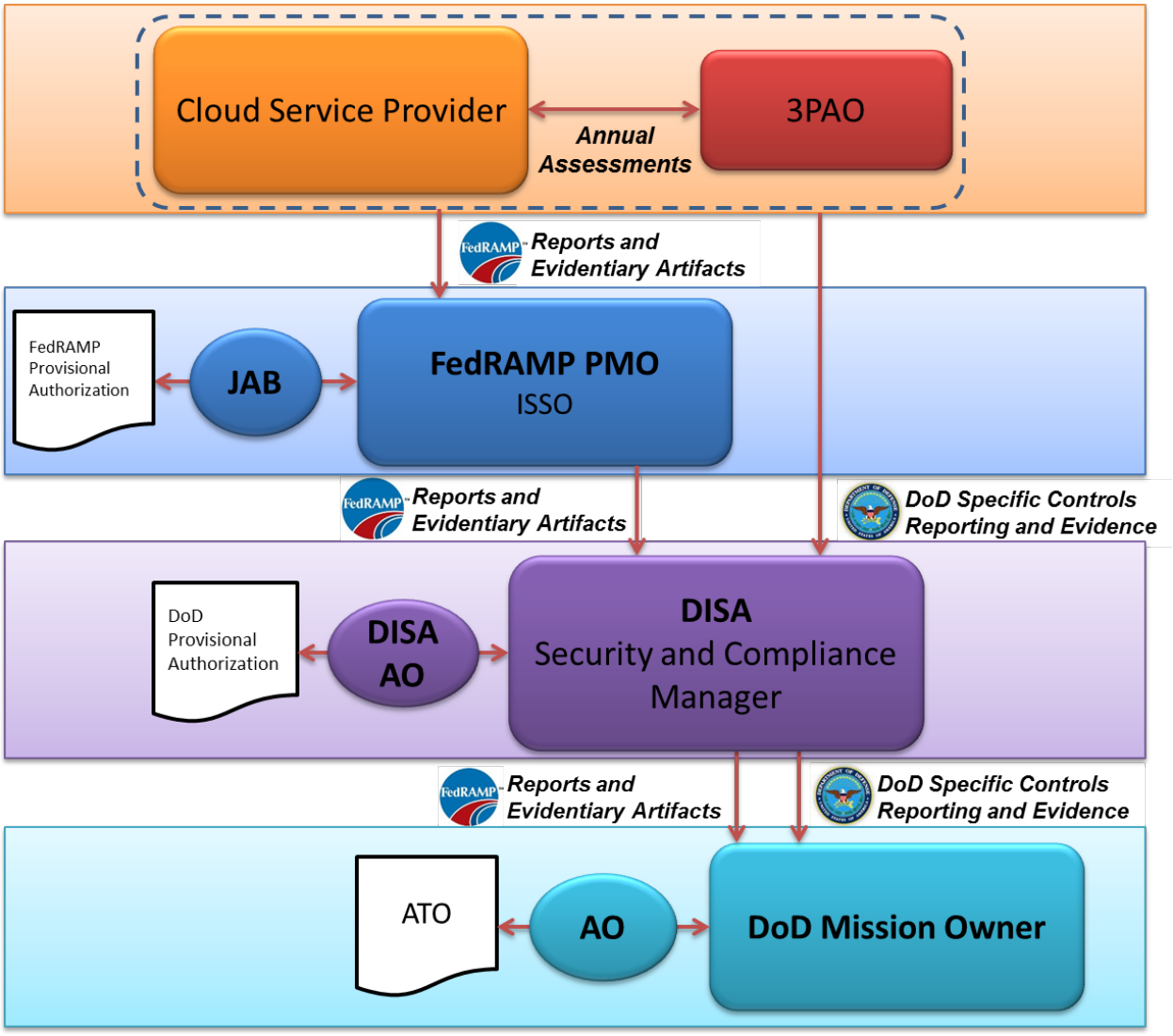

Figure 4 – DoD Continuous Monitoring for CSOs with a FedRAMP JAB PA

Figure 5 shows the flow of continuous monitoring information if the CSO has a 3PAO assessed non-DoD Federal Agency ATO listed in the FedRAMP catalog. Since the FedRAMP JAB does not control the Agency ATO, information may not flow from the CSP to the FedRAMP PMO.

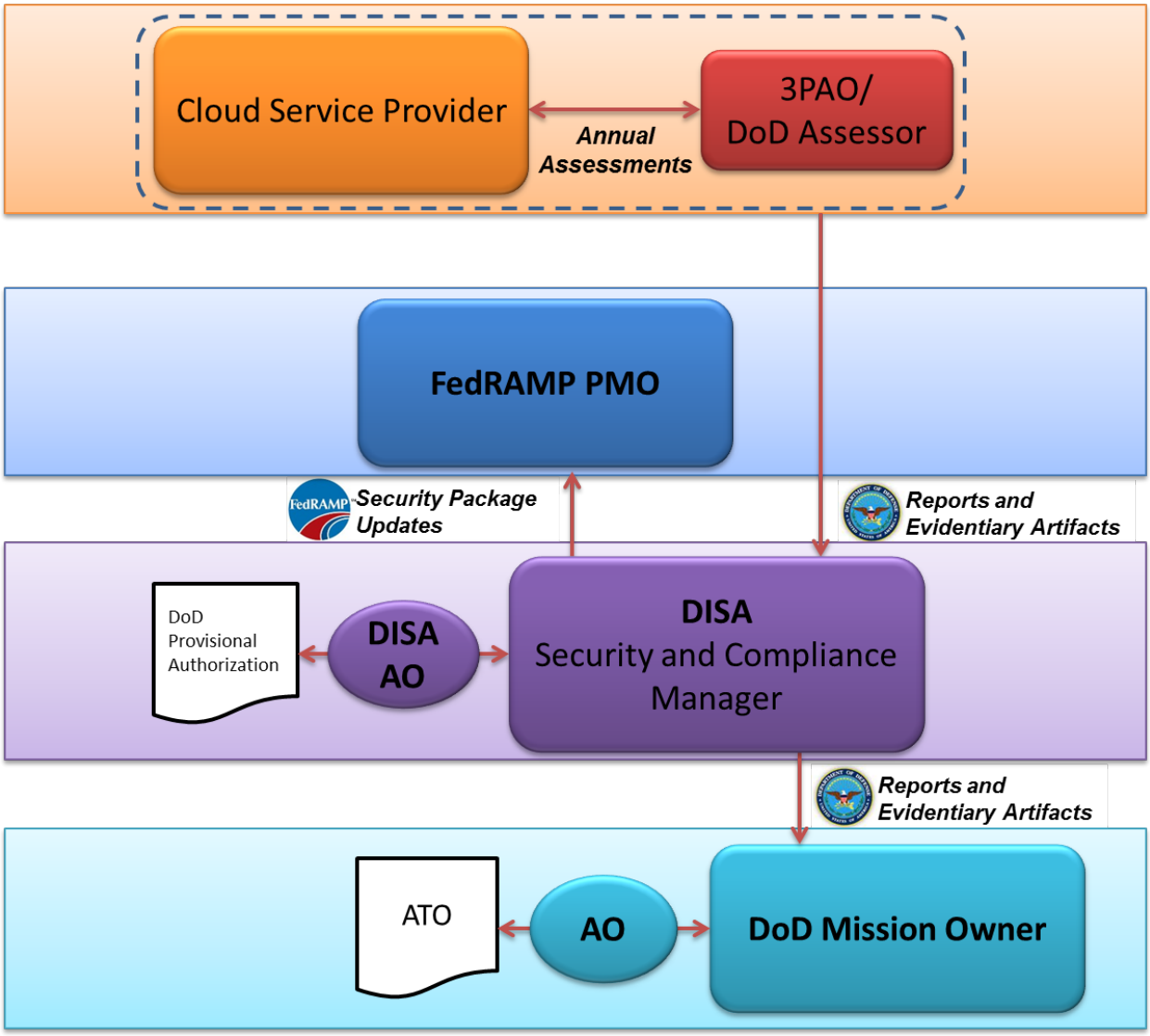

Figure 5 – DoD Continuous Monitoring for FedRAMP CSOs with a 3PAO assessed Non-DoD Federal Agency ATO

5.3.1.2 DoD Assessed CSOs

Figure 6 shows the flow of continuous monitoring information for DoD private/community CSOs that have a DoD PA and ATO, but are not in the FedRAMP catalog. Continuous monitoring will be directed by the DoD RMF, rather than the *FedRAMP Continuous Monitoring Strategy Guide*. As part of the RMF authorization process, CSPs will create a continuous monitoring strategy that meets DoD requirements in the System Security Plan. All reports and artifacts required by that continuous monitoring strategy will be provided by the CSP to DISA. DISA will, in turn, disseminate those artifacts to all Mission Owners utilizing that CSO, the DISA AO, and the Computer Network Defense Service Provider (CDSP) entities as defined in Section 6, *Cyber Defense and Incident Response.*

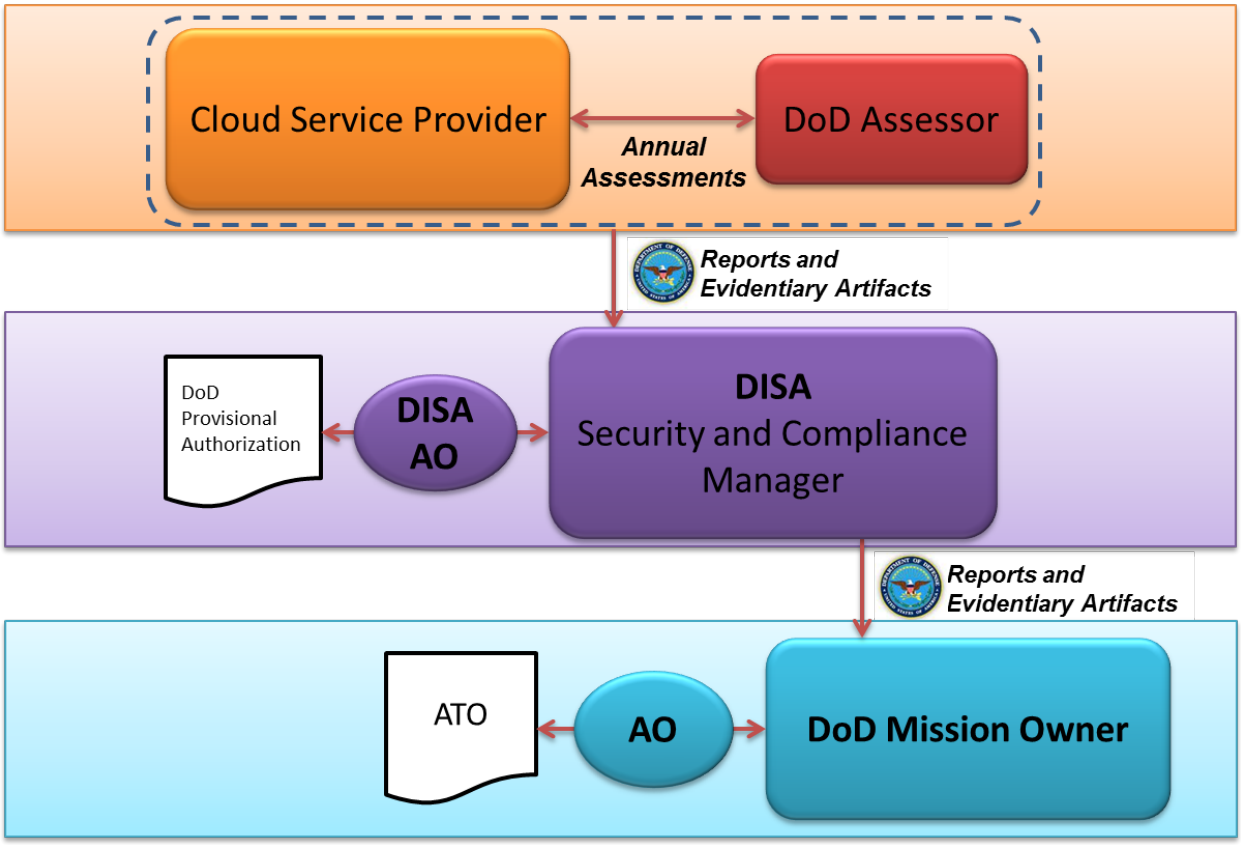

Figure 6 – DoD Continuous Monitoring for DoD Assessed CSOs

5.3.2 Change Control

The DoD change control process for CSOs mirrors that of FedRAMP, with a focus on how changes affect the DoD PA and the security of hosted mission systems/applications and information.

The FedRAMP Continuous Monitoring Strategy Guide, dated June 6, 2014, states:

"Systems are dynamic and FedRAMP anticipates that all systems are in a constant state of change. Configuration management and change control processes help maintain a secure baseline configuration of the CSP's architecture. Routine day-to-day changes are managed through the CSP's change management process described in their Configuration Management Plan.

However, before a planned major significant change takes place, CSP's must perform a Security Impact Analysis, consistent with control CM-4, to determine if the change will adversely affect the security of the system. The Security Impact Analysis is a standard part of a CSP's change control process as described in the CSP's Configuration Management Plan."

As with FedRAMP, CSPs must give DoD 30-day notice prior to major significant changes. If a change is made without approval that affects the risk posture of the system, the DISA AO can revoke the DoD PA. As with continuous monitoring, the change control process will differ for CSPs depending on if they are in the FedRAMP catalog and if they have a DoD assessed PA or ATO. Figure 7, Figure 8, and Figure 9 show these change control processes.

Corresponding Security Controls: CM-3

5.3.2.1 CSOs in the FedRAMP Catalog

The FedRAMP Continuous Monitoring Guide defines a major significant change as a change to the scope of an approved PA or an impact to the authorization boundary of the CSO. The FedRAMP *Significant Change Security Impact Analysis Form* (provided by the FedRAMP ISSO to CSPs reporting a significant change) enumerates major significant changes. The review of major significant changes will be performed at multiple layers, as reflected in Figure 7. As part of the FedRAMP process, when the CSO has a FedRAMP PA, the CSP will notify their AO of any planned major significant change and subsequently provide a Security Impact Analysis for the planned change. The planned change will be reviewed by the ISSO and/or JAB Technical Representatives (TRs), and then forwarded to the JAB for approval. During ISSO review, the DoD JAB TR will inform the FedRAMP ISSO if planned changes will adversely affect the security of the information hosted by the CSO for DoD cloud customers. The DoD JAB TR will notify DISA, who will in turn notify all Mission Owners utilizing that CSO, the DISA AO, and the Cyber Defense Service Provider (CDSP) entities as defined in Section 6, *Cyber Defense and Incident Response.*

When a CSO is included in the FedRAMP catalog, but does not have a JAB PA, the CSP will notify DISA directly in addition to any other required points of contact. (E.g. A CSP with a non-DoD agency ATO would notify both that agency and DISA). This is required because the FedRAMP JAB does not control the Agency ATO, and information may not flow from the CSP to the FedRAMP PMO and DISA. DISA will in turn notify all Mission Owners utilizing that CSO, the DISA AO, and the CDSP entities as defined in Section 6, *Cyber Defense and Incident Response.* The Security Impact Analysis must additionally cover the FedRAMP+ C/CEs. Once informed, DISA will review the proposed change to assess if it will, and ensure it will not, adversely affect the security of the DoD Information Network (DoDIN) as a whole or the DISN with respect to the impact level at which it is authorized. Any updates to the FedRAMP Security Package will be forwarded to DISA.

FedRAMP requires a security assessment be performed by a 3PAO after a major significant change is implemented, with a corresponding Security Assessment Report created. CSPs must

also include all FedRAMP+ C/CEs in post-change assessments to meet DoD requirements. DISA will notify affected Mission Owners of proposed major significant changes and provide its assessment of the change within the scope of the CSO PA. Mission Owners are responsible for assessing the effects of proposed changes for effects that fall within the scope of their SLAs.

Figure 7 shows the normal flow of major significant change information if the CSP has a FedRAMP JAB PA.

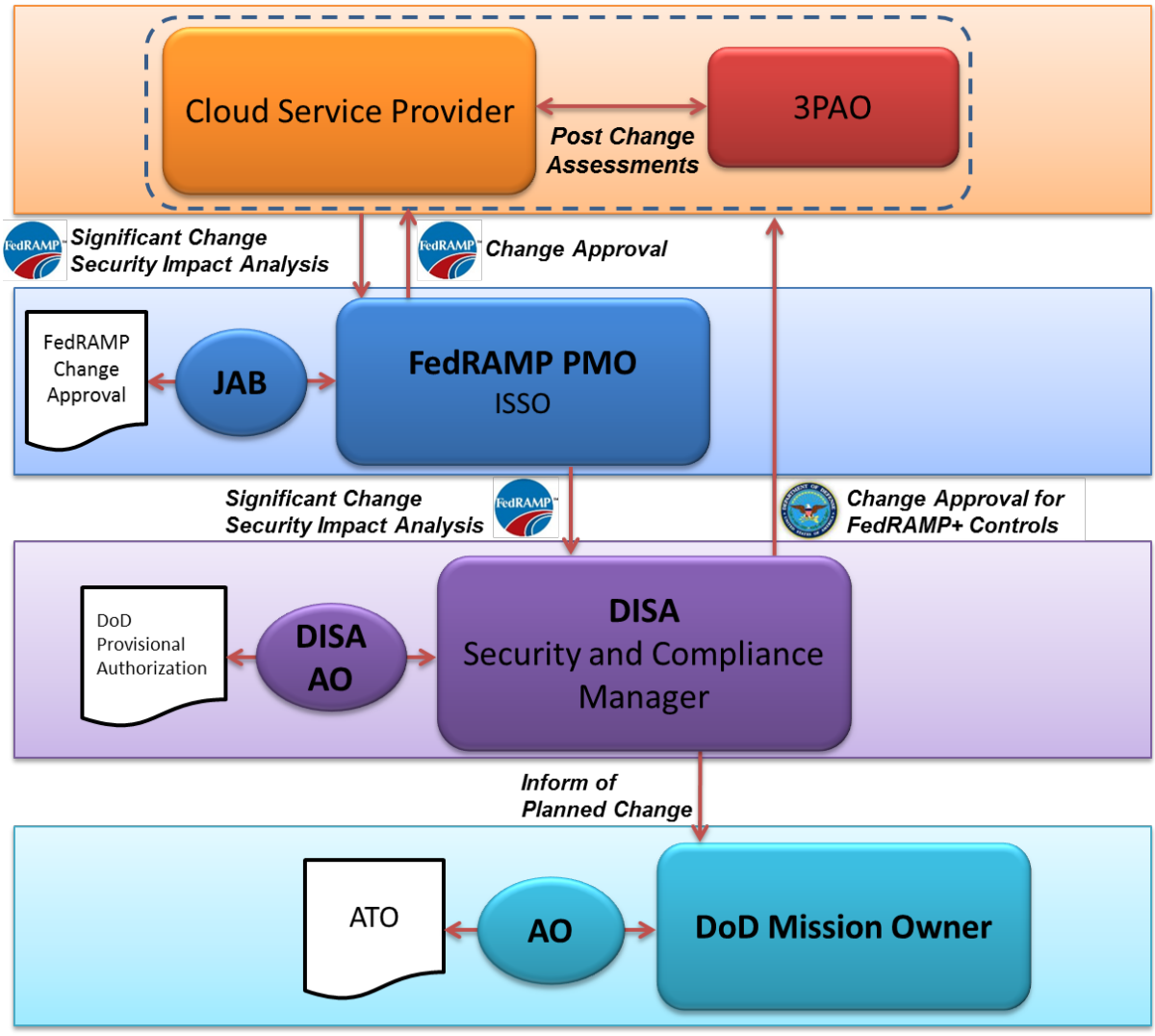

Figure 7 - DoD Change Control Process for CSPs CSOs with a FedRAMP JAB PA

Figure 8 shows the normal flow of significant change information if the CSO has a 3PAO assessed Non-DoD Federal Agency ATO listed in the FedRAMP catalog. Since the FedRAMP JAB does not control the Agency ATO, information from the CSP may not flow from the authorizing agency to the FedRAMP PMO. To avoid the possibility of DoD not being informed of potential changes, CSPs must send change requests to DISA in addition to the authorizing agency.

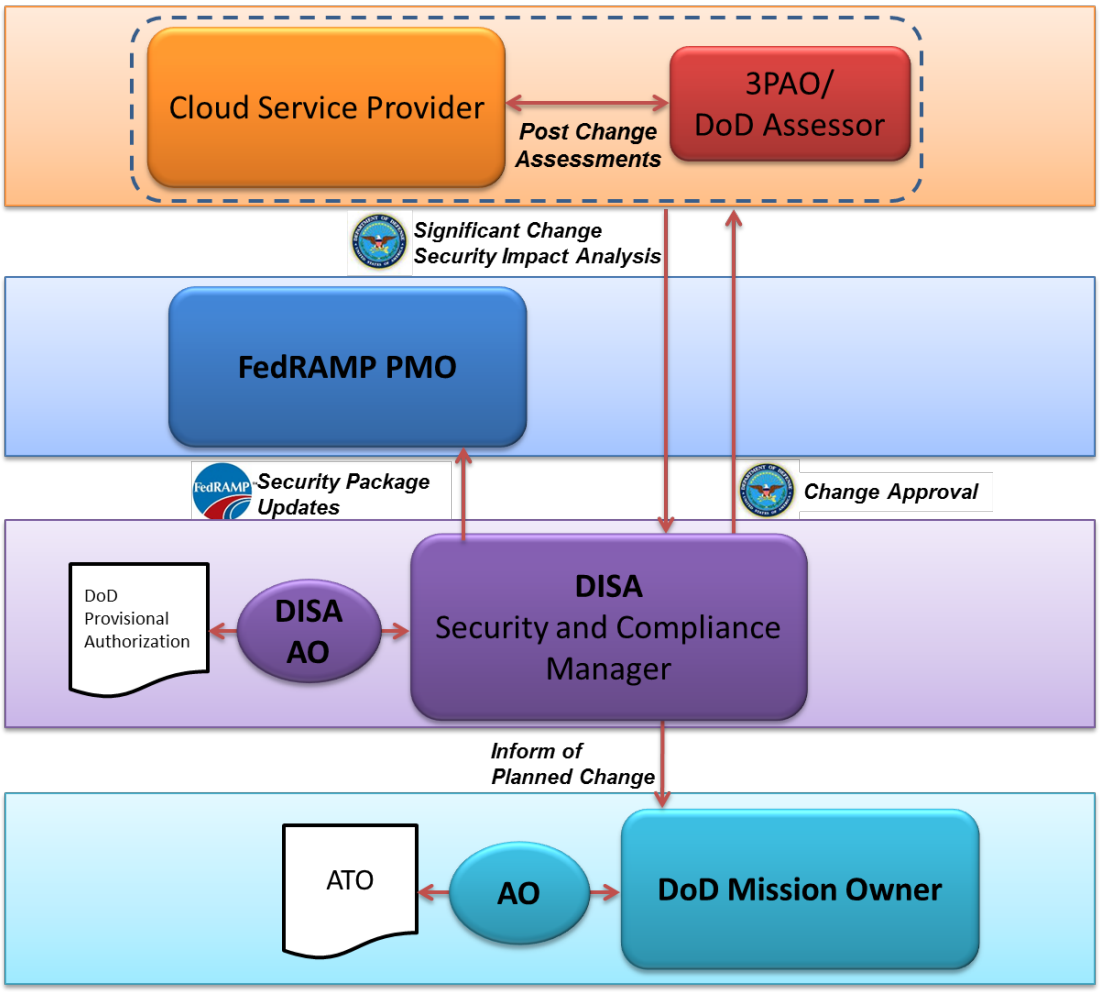

Figure 8 - DoD Change Control Process for FedRAMP CSPs CSOs with a 3PAO assessed Federal Agency ATO

5.3.2.2 DoD Assessed CSOs

Figure 9 shows the flow of significant change for non-FedRAMP CSOs having a DoD PA or ATO assessed by a DoD SCA organization and authorized by a DoD AO. The review of significant change information will be directed by the DoD RMF, rather than the FedRAMP change control process. CSPs will have similar responsibilities, but will report directly to DISA. DISA will, in turn, disseminate those artifacts to all Mission Owners utilizing that CSO, the DISA AO, and the CDSP entities as defined in Section 6, *Cyber Defense and Incident Response.* These entities will review the proposed change to ensure it will not adversely affect the security

posture of the CSO with respect to its PA or ATO. The planned change will also be reviewed by the Mission Owners utilizing the CSO for any adverse impact with regard to their specific usage of the CSO.

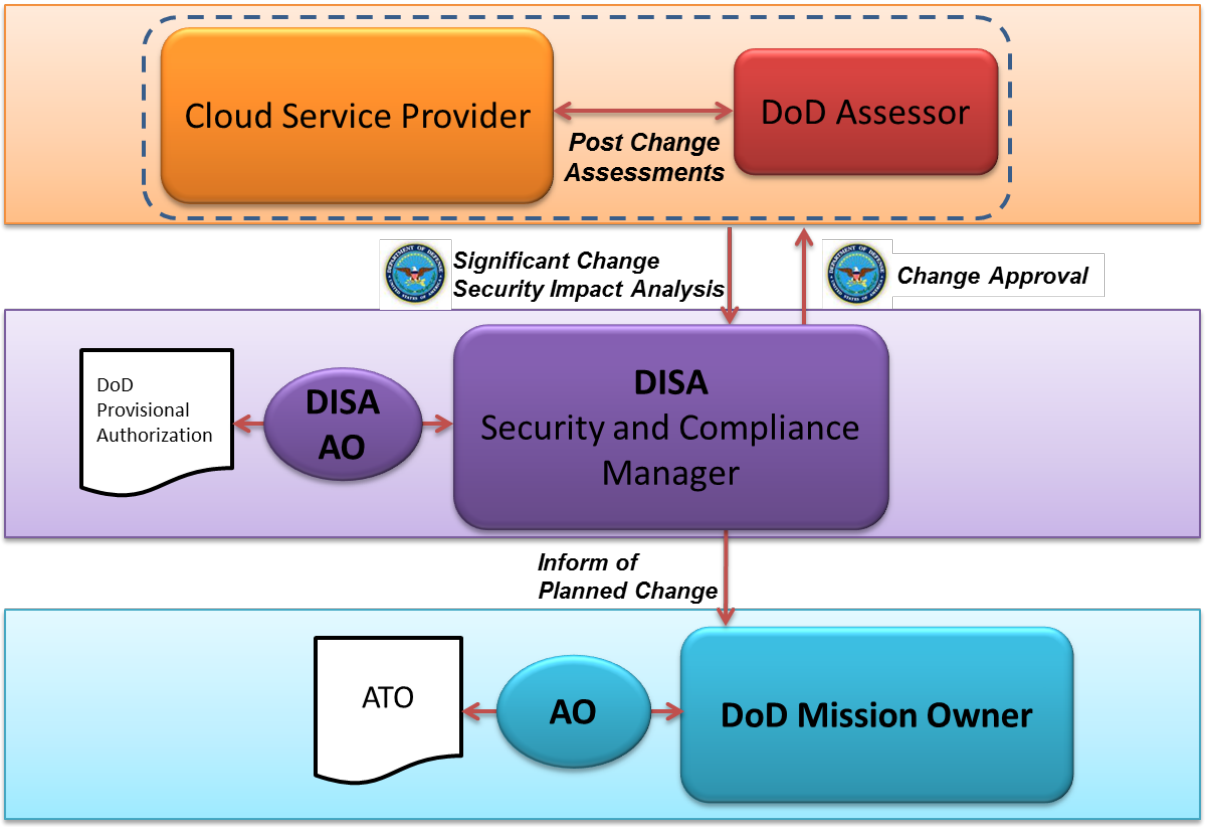

Figure 9 - DoD Change Control Process for DoD Self-Assessed CSPs/CSOs

5.4 CSP use of DoD Public Key Infrastructure (PKI)

In accordance with FedRAMP's selection of IA-2(12) which states "The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials" and the FedRAMP supplemental guidance which states "Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12", CSPs are required to integrate with and use the DoD PKI for DoD entity authentication. (E.g., A web portal that DoD and Federal Government Mission Owner's privileged users log into to configure the CSO.)

The following sections describe how the CSP fulfills its responsibilities with additional detail in the supporting subsections:

Impact Level 2: Whenever a CSP is responsible for authentication of entities and/or identifying a hosted DoD information system, the CSP will use DoD PKI certificates in compliance with DoDI 8520.03. CSPs will enforce the use of a physical token referred to as the "Common Access Card (CAC)" or "Alt Token" for the authentication of DoD privileged users. CSPs must make use of DoD Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) resources for checking revocation of DoD certificates and DoD Certificate Authorities;

and must follow DoD instructions and industry best practices for the management and protection of cryptographic keys.

***Impact Levels 4/5*:** Whenever a CSP is responsible for authentication of entities and/or identifying a hosted DoD information system, the CSP will use DoD PKI certificates in compliance with DoDI 8520.03. CSPs will enforce the use of a physical token referred to as the "Common Access Card (CAC)" or "Alt Token" for the authentication of DoD privileged and DoD non-privileged users. CSPs must make use of DoD OCSP or CRL resources for checking revocation of DoD certificates and DoD Certificate Authorities; and must follow DoD instructions and industry best practices for the management and protection of cryptographic keys. DoD issued PKI server certificates will be used to identify the CSP's DoD customer ordering/service management portals and SaaS applications and services contracted by and dedicated to DoD use.

Impact Level 6: Whenever an on-premises CSO is responsible for authentication of DoD entities and/or identifying a hosted DoD information system, the CSP will use NSS PKI certificates in compliance with DoDI 8520.03 and CNSSP-25. CSPs will enforce the use of a physical token referred to as the CNSS Secret Internet Protocol Router Network (SIPRNet) Hardware Token for the authentication of DoD Mission owner and CSP privileged and non-privileged end users. When implementing NSS PKI, CSPs must make use of NSS OCSP or CRL resources for checking revocation of NSS certificates and NSS Certificate Authorities; and must follow CNSS / NSA instructions for the management and protection of cryptographic keys. CNSS issued PKI server certificates will be used to identify the CSP's DoD customer ordering/service management portals and SaaS applications and services contracted by and dedicated to DoD use.

NOTE: A CSP must PK enable their customer ordering/service management portals for all service offerings and their SaaS service offerings for general DoD user access at levels 4 and up or provide a customer configurable service offering to permit PK enabling and integration with the required PKI. For complete compliance the CSP will integrate with the DoD PKI and the Federal PKI for levels 2 through 5. For Level 6 the CSP will integrate with the NSS (SIPRNet) PKI. Both the DoD and NSS PKI are operated by DISA[50] while the Federal PKI is operated by GSA[51]. PK enabled customer ordering/service management portals may require a separate URL or dedicated application / application interface as best determined by the CSP to meet the Federal Government requirement.

Corresponding Security Controls: IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-2(12), IA-5(2), IA-5(11), IA-7, IA-8

NOTE: NSS PKI and SIPRNet token requirements for off-premises Level 6 CSPs and CSOs need to be coordinated with OUSD(I) and DSS. Associated policies are addressed above in Section 4.2, *Assessment of DoD Cloud Services and Enterprise Services Applications* under the Impact Level 6 topic. Coordinated guidance and requirements for off-premises CSPs and their CSOs for a DoD Level 6 provisional authorization may appear in a future release of the CC SRG. This note applies to all subsections in Section 5.4.

[50] DoD PKI/PKE: http://iase.disa.mil/pki-pke/Pages/index.aspx
[51] Federal PKI: http://www.idmanagement.gov/federal-public-key-infrastructure

5.4.1 Identification, Authentication, and Access Control Credentials

DoDI 8520.03, *Identity Authentication for Information Systems* is the DoD policy that defines the credentials that DoD privileged and non-privileged users must use to identify themselves to DoD information systems to be authenticated before being granted access. It also defines the credentials that DoD information systems use to identify themselves to each other. This is fully applicable to DoD information systems instantiated on cloud services. Additionally, CNSS Policy #25 and CNSSI 1300 provide similar guidance for NSS. For the purpose of this discussion, the process of identification and authentication will be referred to as I&A.

5.4.1.1 Mission Owner Credentials for CSP and Mission System Interfaces

This section defines the Mission Owner access control credentials required at each information impact level IAW DoDI 8520.03 in the following categories:

- Mission Owner privileged user access to the CSP's customer ordering and service management interfaces or portals for all service offerings (IaaS/PaaS, SaaS).
  - Integration with DoD PKI is typically a CSP responsibility. Minimally, the CSP is responsible for providing capabilities that enable Mission Owners to configure a CSP service offering that integrates with DoD PKI.
- Mission Owner Non-privileged user (i.e., mission application end-users) access to CSP SaaS offerings.
  - Integration with DoD PKI is typically a CSP responsibility. Minimally, the CSP is responsible for providing capabilities that enable Mission Owners to configure a CSP service offering that integrates with DoD PKI.
- Non-privileged user access to Mission Owner's systems and applications instantiated on IaaS/PaaS. (i.e., mission application end-users)
  - Implementation is a Mission Owner responsibility.
- Mission Owner privileged user access to their systems and applications instantiated on IaaS/PaaS for the purpose of administration and maintenance.
  - Implementation is a Mission Owner responsibility.

Table 4 lists the Mission Owner credential types required at each impact level for various use cases and the policy under which they are required. The DoD Policy column identifies the authentication methods that Mission Owners must implement for use in the systems and applications they instantiate in a CSP's CSO. This is primarily applicable to IaaS/PaaS. The IA-2(12) column identifies the authentication methods that CSPs must implement for use in the service offerings they provide to their DoD customer. This primarily applies to SaaS and CSP's customer ordering/service management portals.

Table 4 - Mission Owner Credentials

Impact Level	Implemented by Mission Owner IAW DoD policy	Implemented by CSP IAW FedRAMP's selection of IA-2(12):
Level 2	▪ Non-privileged user access to publicly released information requires no I&A, unless the information owner requires it. If required, the Mission Owner	▪ Non-privileged user access to non-publicly released non-CUI and non-critical mission information in the CSP's SaaS offering minimally requires

	determines the type of I&A to be used. ▪ Non-privileged user access to non-publicly released non-CUI and non-critical mission information minimally requires I&A through the use of a User Identifier (UID) and password that meets DoD length and complexity requirements. The Mission Owner is encouraged to require the use of a stronger I&A technology in accordance with the sensitivity of the private information (e.g., UID/Password with two-step verification, two-factor token based onetime password, DoD-approved PKI token/certificate, CAC/PKI, etc.) ▪ Mission Owner Privileged users' access to administer Mission Owner systems/applications instantiated on IaaS/PaaS requires the use of DoD CAC/PKI or Alt Token/PKI.	I&A through the use of a User Identifier (UID) and password that meets DoD length and complexity requirements. The Mission Owner is encouraged to require the use of a stronger I&A technology in accordance with the sensitivity of the private information (e.g., two-factor token based onetime password, DoD-approved[52] PKI token/certificate, CAC/PKI, etc.) ▪ Mission Owner's privileged users' access to the CSP's customer ordering/service management portals for all service offerings requires the use of DoD CAC/PKI or Alt Token/PKI.
Level 4 and 5	▪ Non-privileged user access to CUI, non-CUI critical mission data, and/or unclassified NSS (L5) requires the use of DoD CAC/PKI or other DoD-approved PKI[53]. ▪ Mission Owner Privileged users' access to administer Mission Owner systems/applications instantiated on IaaS/PaaS requires the use of DoD CAC/PKI or Alt Token/PKI.	▪ Non-privileged user access to CUI, non-CUI critical mission data, and/or unclassified NSS (L5) information in the CSP's SaaS offering requires the use of DoD CAC/PKI or other DoD-approved PKI[54]. ▪ Mission Owner's privileged users' access to the CSP's customer ordering/service management portals for all service offerings requires the use of DoD CAC/PKI or Alt Token/PKI.
Level 6	▪ Non-privileged user access to classified information requires the use of NSS SIPRNet Token/PKI. ▪ Mission Owner Privileged users' access	▪ Non-privileged user access to classified information in the CSP's SaaS offering requires the use of NSS SIPRNet Token/PKI. ▪ Mission Owner's privileged users'

[52] DoD-approved PKIs: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx
[53] DoD-approved PKIs: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx
[54] DoD-approved PKIs: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx

	to administer Mission Owner systems/applications instantiated on IaaS/PaaS requires the use of NSS SIPRNet Token/PKI.	access to the CSP's customer ordering/service management portals for all service offerings requires the use of NSS SIPRNet Token/PKI.

NOTE: Mission Owner personnel that are involved in managing any portion of a CSP's service offering or who are able to order services from the CSP (i.e., possesses accounts on the CSP's customer ordering and service management interfaces or portals for any service offering (IaaS/PaaS, SaaS)), are considered Privileged Users by DoD and therefore are required to authenticate using DoD CAC, or Alt Token IAW DoDI 8520.03.

NOTE: It is recognized that some Level 4/5 systems must support some non-privileged user populations (e.g., retirees) that cannot receive a DoD CAC/PKI or other DoD-approved PKI authenticator to gain access to CUI (e.g., PII/PHI) for which they have a legal right to access. In cases such as these the Mission Owner will seek AO approval to categorize such data as Unclassified Sensitivity Level 1 IAW DoDI 8520.03, which would permit the use of Credential Strength A. (E.g. A password as an authenticator) While such populations must typically use a UID and strong password managed IAW DoD password policy, the Mission Owner is encouraged to implement stronger measures such as two-step verification where an access code is sent to the user via a different communications path than the one accessing the web site or application after entering the UID/password combination. In effect, this becomes a two-factor authentication system.

5.4.1.2 CSP Privileged User Credentials

This section defines the I&A and access control credentials that the CSP privileged users must use when administering the CSP's infrastructure supporting Mission Owner's systems.

Impact Levels 2/4*:* IAW the separation requirements for Levels 2 and 4 described in Section 5.2.2.1, *Impact Level 2 Location and Separation Requirements,* and 5.2.2.2 ,Impact *Level 4 Location and Separation Requirements,* and FedRAMP's selection of IA-2(1) and IA-2(3), the CSP must minimally implement two factor authentication for CSP privileged user access to administer and maintain CSP infrastructure supporting Federal and DoD contracted services. While the best practice of using a hardware token technology implementing a multi-factor one-time password or PKI certificate technology solution similar to DoDI 8520.03 Credential Strength D is preferred, these identity credentials minimally use a multi-token solution or a multi-factor one-time password solution similar to DoDI 8520.03 Credential Strength C.

Impact Level 5: IAW the separation requirements for Level 5 described in Section 5.2.2.3, *Impact Level 5 Location and Separation Requirements* and DoD policy, the CSP must implement a strong two-factor I&A capability for CSP privileged user access to administer and maintain dedicated CSP infrastructure supporting Federal and DoD contracted services. The strong two-factor I&A capability must be dedicated to the dedicated CSP infrastructure. These identity credentials minimally use a hardware token technology implementing a multi-factor one-time password or PKI certificate technology solution similar to DoDI 8520.03 Credential Strength D.

NOTE: While DoDI 8520.03 requires that all administrators of DoD or partner managed systems use identity Credential Strength E (i.e., hardware token PKI technology issued by an identity

credential service provider that is either a Federal agency, an approved shared service provider under the Federal PKI Policy Authority Program, or an identity credential service provider that has been specifically approved by the DoD CIO as a Credential Strength E service provider e.g., DoD CAC or ALT) for privileged access to DoD systems, DoD is not enforcing this requirement on CSP infrastructure administrators / privileged users managing CSP assets at this time.

Impact Level 6*:* IAW the separation requirements for Level 6 described in Section 5.2.2.4, *Impact Level 6 Location and Separation Requirements* and CNSS policy, the CSP must implement SIPRNet Token/PKI authentication for CSP privileged user access to administer and maintain dedicated CSP infrastructure supporting Federal and DoD contracted Level 6 services connected to SIPRNet.

5.4.2 Public Key (PK) Enabling

Public Key (PK) enabling refers to the process through which hosts and applications are enabled to hold or use PKI certificates for the following:

- Identifying themselves to other hosts.
- Establishing secure communications paths.
- Accepting DoD PKI certificates for system and user authentication.
- Validating the validity of PKI certificates while making use of the DoD OCSP responder resources and/or CRL resources.

The IASE web site page Public Key Infrastructure (PKI) and Public Key Enabling (PKE)[55] provides information needed to PK-enable Mission Owner's systems/applications instantiated on CSP's IaaS/PaaS offerings and CSP's PK-enabling of SaaS offerings and service ordering/management portals/interfaces.

5.5 Policy, Guidance, Operational Constraints

DoD-specific policy, guidance and operational constraints must be followed as appropriate by CSPs. DISA will evaluate CSP submitted equivalencies to any specific security control, SRG, or STIG requirement on a case by case basis.

5.5.1 SRG/STIG Compliance

Mission Owners must utilize all applicable DoD SRGs and STIGs to secure all Mission Owner systems and applications instantiated on CSP's IaaS and PaaS at all levels.

CSP's CSOs are subject to the FedRAMP selected SP 800-53 security control CM-6. This is applicable to all infrastructure, hardware and software, which constitutes and supports the CSP's CSO whether it is IaaS, PaaS, or SaaS. CSOs are assessed under FedRAMP in accordance with the security configuration checklists specified in the FedRAMP value.

All STIGs and SRGs can be found on DISA's IASE web site[56] along with an SRG/STIG Applicability Guide[57].

[55] DoD PKI/PKE: http://iase.disa.mil/pki-pke/Pages/index.aspx
[56] STIGs and SRGs: http://iase.disa.mil/Pages/index.aspx
[57] SRG/STIG Applicability Guide: http://iase.disa.mil/stigs/agct/Pages/index.aspx

DoD recommends that STIGs and/or SRGs be used to fulfill the CM-6 baseline configuration requirement for systems that support DoD systems as follows:

Impact Level 2: While the use of STIGs and SRGs is preferable, industry standard baselines such as those provided by the Center for Internet Security are an acceptable alternative to the STIGs and SRGs.

Impact Levels 4/5/6: STIGs are applicable if the CSP utilizes the product a STIG addresses. SRGs are applicable in lieu of STIGs if a product specific STIG is not available. However, the SP 800-53 control applies whether or not a STIG or SRG is available.

For dedicated infrastructure that only serves DoD tenants, CSPs must utilize all applicable DoD STIGs and/or SRGs to secure all DoD contracted cloud computing services. This applies at levels 4 and above for IaaS, PaaS, and SaaS offerings.

Corresponding Security Controls: CM-6

5.6 Physical Facilities and Personnel Requirements

The following sections discuss facility and personnel requirements as they align to the impact levels.

5.6.1 Facilities Requirements

Impact Level 2: CSP data processing facilities supporting Level 2 information will meet the physical security requirements defined in the FedRAMP Moderate baseline.

Impact Levels 4 and 5: CSP data processing facilities supporting Level 4 and 5 CSOs/information will meet the physical security requirements defined in the FedRAMP Moderate baseline as well as any FedRAMP+ C/CEs related to physical security.

Impact Level 6: DoD data **on-premises** processing facilities that support cloud services infrastructure and classified service offerings will be housed in facilities (designated as a secure room) designed, built, and approved for open storage commensurate with the highest classification level of the information stored, processed, or transmitted as defined in DoDM 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*[58].

5.6.2 CSP Personnel Requirements

The concept of cloud operations, given the shared responsibilities between multiple organizations along with the advanced technology being applied within this space, can impact personnel security requirements. The ability for a CSP's personnel to alter the security controls/environment of a provisioned offering and the security of the system/application/data processing within the offering may vary based on the processes/controls used by the CSP. The components of the underlying infrastructure (e.g., hypervisor, storage subsystems, network devices) and the type of service (e.g., IaaS, PaaS, SaaS) provided by the CSP will further define the access and resulting risk that CSP's employees can pose to DoD mission or data. While CSP personnel are typically not approved for access to customer data/information for need-to-know

[58] DoDM 5200.01 Vol3: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

reasons (except for information approved for public release), they are considered to be able to gain access to the information through their duties.

Access to DoD information at the various levels above Level 2 is limited by national affiliation. For other than US Citizens or Non-Citizen US Nationals as defined in 8 U.S. Code § 1408[59], national affiliation is defined in 22 CFR 120.15[60] – US person and 120.16 – Foreign person.

The limitations by Information Impact Level are as follows:

Impact Level 2: CSP personnel having access to the systems processing/storing DoD public information may be US Citizens, US Nationals, US persons, or Foreign persons. i.e., there is no restriction.

Impact Level 4/5: CSP personnel having access to the systems processing/storing DoD CUI information or to the information itself at Impact Level 4/5 must be US Citizens, US Nationals, or US Persons. No Foreign persons may have such access.

Impact Level 6: CSP personnel having access to systems processing/storing classified information or to the information itself must be US Citizens.

Corresponding Security Controls: PS-2, PS-3

5.6.2.1 CSP Personnel Requirements – PS-2: Position Categorization

The FedRAMP Moderate baseline includes the personnel security controls PS-2, PS-3, and enhancement PS-3(3). Under PS-2, the CSP is required to "assign a risk designation to all organizational positions" and "Establish screening criteria for individuals filling those positions". Supplemental guidance states "Position risk designations reflect Office of Personnel Management (OPM) policy and guidance." The OPM position designation process takes into account the duties, level of supervision, and the scope over which misconduct might have an effect (i.e., worldwide/government-wide, multi-agency, or agency). For IT system and information access it also takes into account the sensitivity level of the information accessed (i.e., non-CUI, CUI, and classified).

The OPM *Position Designation System* October 2010 document[61] and OPM *Position Designation Tool*[62] are provided to enable Federal Agencies a methodical and consistent means to determine position sensitivity for National Security Positions (e.g., positions concerned with the protection of the Nation from foreign aggression or espionage or positions that require regular access to classified information) and Public Trust Positions (e.g., positions at the high or moderate risk levels, which includes responsibility for protection of information security systems). Position risk levels are determined using the Position Designation Tool. A position may have both National Security and Public Trust considerations that will jointly impact the

[59] 8 U.S. Code § 1408: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title8/pdf/USCODE-2010-title8-chap12-subchapIII-partI-sec1408.pdf
[60] 22 CFR 120.15, 120-16: https://www.gpo.gov/fdsys/pkg/CFR-2011-title22-vol1/pdf/CFR-2011-title22-vol1-sec120-15.pdf
[61] OPM Position Designation System document: http://www.opm.gov/investigations/background-investigations/position-designation-tool/oct2010.pdf
[62] OPM Position Designation Tool: http://www.opm.gov/investigations/background-investigations/position-designation-tool/

sensitivity level and ultimately the type of security investigation required. The Position Sensitivity Tool will be used to determine position sensitivity, position risk levels and investigation requirements for key CSP personnel.

DoD's primary concern is CSP personnel with direct access to or the ability to gain access to DoD information, or that have responsibilities that can affect the security of the information technology processing, storing, or transmitting that information. Under OPM policy, such a person with access to CUI or classified information is designated as filling a position designated as "critical-sensitive" or "high risk". However, if the person's "work is carried out under technical review of a higher authority" (i.e., a person holding a "critical-sensitive" or "high risk" position), then the position may be designated as "noncritical-sensitive" or "moderate risk". Positions only having access to non-CUI and publicly released information could have a designation of "non-sensitive" or "low risk". All positions are considered to have some level of "public trust".

From a DoD policy perspective under PS-2 and IAW DoD 5200.2-R, *Personnel Security Program*[63] Category I automated data processing (ADP) (ADP-1 or IT-1), positions include those in which an individual is responsible for the planning, direction, and implementation of a computer security program; has major responsibility for the direction, planning and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way and with a relatively high risk for causing grave damage or realize a significant personal gain. These positions are designated "critical-sensitive". Category II automated data processing (ADP) (ADP-2 or IT-2) positions include those in which an individual may have the same responsibilities listed for ADP-1 but whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system. These positions are designated "noncritical-sensitive". These designations are consistent with the OPM Position Designation System document and automated tool.

To receive a DoD PA, the CSP must demonstrate that their personnel position categorization and compliance with PS-2 is equivalent to the OPM position designations for the similar CSP positions to the "critical-sensitive" (e.g., DoD's ADP-1) or "high risk"; "noncritical-sensitive" (e.g., DoD's ADP-2) or "moderate risk"; and/or "non-sensitive" or "low risk" (i.e., access to only non-CUI and public information) position designations. These designations drive the level of screening to be established IAW the second half of PS-2 and for PS-3.

5.6.2.2 CSP Personnel Requirements – PS-3: Background Investigations

Under PS-3 and PS-3(3), the CSP is required to "Screen individuals prior to authorizing access to the information system", and re-screen IAW an organizational defined frequency. PS-3(3) addresses "additional personnel screening criteria" for information "requiring special protection" such as CUI.

Per the FedRAMP supplemental guidance for PS-3, found in the *FedRAMP Control Specific Contract Clauses v2*, June 6, 2014 document[64], an agency must stipulate, "IAW OPM and OMB requirements", the type of background investigation required for CSP personnel having access to

[63] DoD 5200.2-R : http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf
[64] FedRAMP Control Specific Contract Clauses v2, June 6, 2014; http://cloud.cio.gov/document/control-specific-contract-clauses

or who can gain access to information. For DoD, the minimum designations are defined by level as follows:

Impact Level 2: CSP personnel supporting Level 2 cloud service offerings will meet the personnel security requirements and undergo background checks as defined in OPM policy IAW the FedRAMP Moderate baseline. As such the minimum background investigation required for CSP personnel having access to Level 2 information based on a "non-sensitive" or "low risk" position designation (i.e., position only has access to public and non-CUI non-critical mission information), is a National Agency Check and Inquiries (NACI). The position sensitivity or risk level and resulting investigation may be elevated beyond the minimum requirement as determined by the Mission Owner / AO, based on additional risk considerations. For instance if the Confidentiality, Integrity or Availability (CIA) of information is determined to be based on a "noncritical-sensitive" or "moderate risk" position using the tool, a National Agency Check with Law and Credit (NACLC) (for "noncritical-sensitive" contractors), or a Moderate Risk Background Investigation (MBI) (for "moderate risk" positions) may be required.

Impact Levels 4/5: CSP personnel supporting Level 4 and 5 cloud service offerings will meet the personnel security requirements and undergo background checks as defined in OPM policy IAW the FedRAMP Moderate baseline, the FedRAMP+ CEs related to personnel security, and DoD personnel security policies. As such the minimum background investigation required for CSP personnel having access to Level 4 and 5 information based on a "critical-sensitive" (e.g., DoD's ADP-1) position designation, is a Single Scope Background Investigation (SSBI) or a Background Investigation (BI) for a "high risk" position designation. The minimum background investigation required for CSP personnel having access to Level 4 and 5 information based on a "noncritical-sensitive" (e.g., DoD's ADP-2) is a National Agency Check with Law and Credit (NACLC) (for "noncritical-sensitive" contractors), or a Moderate Risk Background Investigation (MBI) for a "moderate risk" position designation.

To receive a DoD PA for Level 2, 4, or 5, the CSP must comply with the investigation requirements as listed for personnel requiring access to systems and data (e.g., above the hypervisor). Personnel who have access to the CSP infrastructure (e.g. at the hypervisor or below) must comply with OPM investigation requirements or the CSP must demonstrate that their personnel background investigations and compliance with PS-3 and PS-3(3) are consistent with OPM investigation requirements for each position designation.

NOTE: DoD suggests that the CSP request equivalent investigations to those noted above from an investigation contractor listed on the GSA Federal Acquisition Service Contractor Listing for Category 595 27 HR Support: Pre-Employment Background Investigations web site.[65] In using such a contractor and requesting equivalent investigations the CSP can demonstrate equivalency toward receiving a DoD PA, and preparing for the needed investigations following contract award.

Impact Level 6: In accordance with PS-3(1), invoked by the CNSSI 1253 Classified Information Overlay, personnel having access to a secure room, the infrastructure supporting classified processing, or handling classified information, in addition to meeting the public trust position

[65] GSA Investigation Contractors: http://www.gsaelibrary.gsa.gov/ElibMain/sinDetails.do?executeQuery=YES&scheduleNumber=738+X&flag=&filter=&specialItemNumber=595+27

suitability/investigation requirements (e.g., a favorably adjudicated SSBI for a system administrator in a DoD ADP-1 position) must have a security clearance at the appropriate level. Systems and network administrators (i.e., privileged users), while typically not approved to handle classified information for need-to-know reasons, are considered to have access to classified information through their duties. Therefore these individuals require a clearance at the appropriate level for the classified information stored, processed, or transmitted.

DoD personnel clearances are granted through DoD processes as defined in DoDI 5200.02[66] and the DoD 5200.2-R[67], both entitled *DoD Personnel Security Program (PSP)*. Commercial CSPs' personnel clearances are granted through the Industrial Personnel Security Clearance Process[68].

Contracts for both on-premises and off-premises Level 6 CSOs will include language related to the contractor requiring access to classified information IAW 48 Code of Federal Regulations (CFR) Subpart 4.4 - Safeguarding Classified Information within Industry[69] and Federal Acquisition Regulations (FAR) section 52.204-2 - Security Requirements[70]. Such contractors are required to comply with NISP policies as discussed as cited above WRT organizational facilities clearances and cleared personnel.

To receive a DoD PA for Level 6, the CSP must either have a facility clearance and cleared personnel who will manage the CSO (including top level corporate management), or demonstrate the ability to meet the requirements for such, as defined in Industrial Personnel Security Clearance Process.

For on-premises Level 6 CSOs facilities and personnel clearances will be handled as with any other DoD contract where the contractor needs access to classified information or as required for other purposes.

For off-premises Level 6 CSO facilities and personnel clearances, will be handled through the contracting process as with any other Defense Industrial Base (DIB) contractor. This process is the purview of OUSD(I) and DSS.

5.6.2.3 Mission Owner Responsibilities Regarding CSP Personnel Requirements

In addition to the above requirements, the FedRAMP Control Specific Contract Clauses v2[71], also states the following: "Agencies leveraging FedRAMP Provisional Authorizations will be responsible for conducting their own Background Investigations and or accepting reciprocity from other agencies that have implemented Cloud Service Provider systems." It also states Agencies are responsible for the screening process, and may want to stipulate additional screening requirements. As part of the FedRAMP+ assessment, the processes used by the CSP will be evaluated and discussed in the PA as appropriate. DoD Components and/or Mission

[66] DoDI 5200.2: http://www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf
[67] DoD 5200.2-R: http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf
[68] Industrial Personnel Security Clearance Process: http://www.dss.mil/psmo-i/indus_psmo-i_process_applicant.html
[69] 48 CFR Subpart 4.4:
https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4-subpart4-4
[70] FAR 52.204-2:
https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf
[71] FedRAMP Control Specific Contract Clauses v2, June 6, 2014; https://www.fedramp.gov/resources/documents/

Owners must review the investigation type required for all position designations and address investigation requirements as well as funding in their contracts with the CSP.

5.6.2.4 Training Requirements

DoD 8570.01-M, Information Assurance Workforce Improvement Program, Change 3, January 24, 2012[72] describes the DoD IA Workforce Improvement Program. This manual requires DoD IA personnel to be categorized and sets experience, training, and certification standards. DoD CSPs and Mission Owners must comply with DoD 8570.01-M.

CSPs operating at impact level 6 are also required to meet the requirements of DoD 8570.01-M for their personnel. However, non-DoD CSPs at impact levels 2-5 are not subject to these requirements. CSPs at all impact levels are however, required to train security personnel as described in security control AT-3. The determination to not levy DoD 8570.01-M on commercial CSPs is based on the complexities of attempting to change how a commercial CSP that serves customers outside of DoD hires and trains personnel. Commercial CSP security personnel training will be assessed for compliance with security control AT-3 as part of the FedRAMP and DoD PA assessments.

5.7 Data Spill

Per CNSSI 4009, *CNSS Glossary*[73], a data spill or "spillage" is an unauthorized transfer of classified information or Controlled Unclassified Information to an information system that is not accredited for the applicable security level of the data or information.

A data spill is a cyber-incident that requires immediate reporting and response from both the Mission Owner and CSP in order to minimize the scope of the spill and the risk to DoD data. Mission owners will report the incident via their normal channels; the CSP must report the spill to the mission/information owner as well as follow the requirements in section 6.4 *Cyber Incident Reporting and Response*. While the Mission Owner will most likely detect a spillage within their own dataset, the CSP might also detect a spillage. CSP detection may depend on a particular service offering where the CSP might have intentional access to the content of a Mission Owner information system.

Cloud environments present a unique challenge for data spill response. Data spills are typically remediated or "cleaned" by sanitizing affected hardware to ensure that reconstruction of spilled data is impossible or impractical. This process requires access to physical storage media and frequently involves storage resources being taken offline until the cleanup is complete. Such loss of availability is not acceptable in a cloud environment with multiple tenants sharing the same infrastructure. CSP use of storage virtualization can generate numerous, dynamic instantiations of data and makes physical data locations difficult to ascertain. This makes physical sanitization methods non-viable for data spill remediation in cloud services.

These challenges require a method for mitigating data spill cyber incidents that occur in the cloud. Cryptographic erase described in Section 5.11.1, *Cryptographic Erase*, provides such a method. Cryptographic erase is a high-assurance way of ensuring data at rest can no longer be

[72] DoD 8570.01-M: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
[73] CNSSI 4009: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

read. CE is faster and more practical than physical sanitization methods in large-scale virtualized environments used by cloud services. Further, DoD control of encryption keys permits mission owners to address data spill incidents without alerting the CSP to the presence of unauthorized data.

However, CE is only an option for data that is encrypted. Mission owners should ensure all data is encrypted at rest consistent with Section 5.11, *Encryption of Data-at-Rest in Commercial Cloud Storage.*

Upon discovery of a data spill, mission owners should cryptographically erase unauthorized data by deleting the associated decryption key(s), consistent with NIST SP 800-88 Rev 1. Mission owners must also take any necessary steps to remove unauthorized data that may exist in an unencrypted state, such as in memory of a running VM.

Due to data backup and disaster recovery methods used by Mission Owners and CSPs, data spills could affect associated storage. Data spills remediation must extend to storage media where the spilled data might migrate. All backups and mirrored storage affected by the spill must be remediated. Mission owners are responsible for ensuring that all copies of spilled data are cryptographically erased. Timely detection, reporting, and response are key to limiting the migration of spilled data under these circumstances.

Data spills that involve unauthorized data being stored in an unencrypted state in a CSO must be mitigated by the Mission Owner utilizing any available option to make such data unrecoverable. The response to such an event will likely be limited to methods that provide less assurance than cryptographic erase. Mission Owners that do not or cannot utilize encryption at rest must create data spill response procedures that enumerate all data erasure options in a given CSO. Upon discovery of such an incident, a risk analysis should be performed to determine the best course of action to mitigate the risk of reconstruction of unauthorized data. This may or may not include alerting the CSP to the presence of unauthorized data in order to gain cooperation in mitigating the incident.

Alternate innovative methods for cloud data spill protection/remediation will be assessed for equivalency to standard methods and approved if found sufficient.

Corresponding Security Controls: IR-9, MP-6

5.8 Data Retrieval and Destruction for Off-boarding from a CSO

Off-boarding is the set of activities that take place when a Mission Owner terminates use of a CSO. An off-boarding process is required when a Mission Owner migrates to a new cloud service, a mission reaches end of life, a contract ends, or a CSP ceases operations. The off-boarding process is split into two stages: 1- data retrieval/migration and 2- data sanitization or destruction. Mission owners must prepare for an eventual CSO off-boarding, and CSPs must support the capability in a timely manner.

Upon request by the Mission Owner, the CSP will make all Mission Owner data stored in a CSO available for electronic transfer out of the CSP environment in a standard, non-proprietary format. CSPs must also make available all audit logs relevant to the Mission Owner's use of the CSO. This includes all audit content specified by the AU-2 security control for the time period specified by AU-11. See Section 5.2.3, *DoD Data Ownership and CSP Use of DoD Data* for additional information. CSOs that enable Mission Owners to download their data on demand

and delete or request destruction of data may not require specific CSP action to fulfill this requirement. Each Mission Owner may also request different means of data transfer (for example, as called out in the SLA), at its discretion.

Cryptographic Erase, described in Section 5.11.1, *Cryptographic Erase*, provides a high-assurance way of ensuring data at rest can no longer be read. Upon successful transfer of data out of a CSO, mission owners with data that is encrypted at rest must cryptographically erase all such mission data and take action to ensure that no data remains in the CSO in an unencrypted state. All backups maintained in the CSO's infrastructure, from which the Mission owner is departing, must also be cryptographically erased. Mission owners should also request that all mission data be deleted or made logically inaccessible as per normal CSP procedure for departing customers. Upon verification of successful Mission Owner transfer of data, CSPs must immediately delete or otherwise make all Mission Owner data irretrievable. CSPs remain responsible for sanitizing or destroying all storage devices that held DoD data at the hardware's end-of-life, even after off-boarding is complete IAW Section 5.9, *Reuse and Disposal of Storage Media and Hardware.*

DoD Mission Owners using non-DoD service offerings must be capable of migrating their data at any time. This means that mission owners must have the ability to receive their data from a cloud service on short notice. This capability can be supported in the form of available local storage infrastructure, or a cloud service offered by a different CSP capable of accepting data in a short time frame. This is to ensure that mission owners can quickly retrieve their data in case of a sudden shutdown of a CSO. (e.g. A CSP declares bankruptcy and plans to shut down services). This concern is also mitigated by the mission owner's use of effective backup procedures as described in Section 5.12, *Backup.*

Corresponding Security Controls: DM-2, MP-6

5.9 Reuse and Disposal of Storage Media and Hardware

CSPs will ensure that no residual DoD data exists on all storage devices decommissioned and disposed of, reused in an environment not governed by an agreement between the CSP and DoD, or transferred to a third party; as required by the FedRAMP selected security control MP-6.

Impact Levels 4/5: CSPs may not reuse or dispose of storage hardware until all DoD data has been successfully removed. The CSP will minimally ensure this by "Purging" all data on devices prior to decommissioning, disposal, reuse, or transfer, in accordance with NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*[74]. Devices that are unable to be cleared or purged must be physically destroyed, as defined in NIST SP 800-88 Rev 1. When there is any doubt to the success of the cleared or purged process, the storage device must be destroyed in accordance with NIST SP 800-88 Rev 1.

Impact Level 6: **On-premises** CSP's may not dispose of or reuse storage hardware at a lower sensitivity or classification level but will ensure classified data is irretrievable from

[74] NIST SP 800-88: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

decommissioned devices by sanitizing them in accordance with NSA/CSS Storage Device Declassification Manual 9-12[75].

Corresponding Security Controls: DM-2, MP-6

5.10 Architecture

This section of the CC SRG provides guidance on the various architectural considerations related to DoD's use of DoD and commercial cloud services in the following areas:

- The connection between the CSP's infrastructure/network and the DISN
- CSP service protections and integration into required DoDIN Cyber Defense and access control services
- Mission system/application protections and integration into required DoDIN Cyber Defense and access control services

5.10.1 Cloud Access Point (CAP)

The 15 December 2014 DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services*, states "Commercial cloud services used for Sensitive Data must be connected to customers through a Cloud Access Point (CAP)."

For the purpose of this SRG, Sensitive Data as referenced in the in the DoD CIO memo means CUI as handled at Levels 4/5 or Classified up to SECRET information as handled at Level 6.

A DoD Cloud Access Point (CAP) is a system of network boundary protection and monitoring devices, otherwise known as an IA stack, through which CSP infrastructure and networks will connect to the NIPRNet. A BCAP does not provide for direct internet access to or by Level 4/5 CSP CSOs or other NIPRNet users.

The primary purpose of a NIPRNet CAP is the protection of the DISN from and detection of unauthorized DISN access from the CSP's infrastructure, CSO management plane, CSP corporate networks, CSP connections to the Internet, and from compromised Mission Owner systems/applications and virtual networks. The secondary purpose is to the protection of the DoDIN and DoD information in general by facilitating protected connections for NIPRNet users (and Internet users for internet facing applications) to access Level 4/5 Mission Owner systems/applications instantiated on IaaS/PaaS (or using SaaS) without exposing such traffic to the Internet. These purposes also apply to any other CAP on any other Mission Partner or COI network for the protection of those networks and the sensitive information they contain.

CAP architecture will change depending on whether the cloud infrastructure is on-premises or off-premises. There are internal CAPs (ICAPs) and DISN/NIPRNet Boundary CAPs (BCAPs). Some CAPs will leverage existing infrastructure and some will be a new capability.

In general, the BCAP will provide the following protections:

- Provides DISN perimeter defenses and Boundary Cyber Defense sensing for traffic to and from applications hosted in the cloud service.

[75] NSA/CSS 9-12: https://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf

- Protects DoD missions [within the DISN] along with the DISN and its network services from incidents that affect a particular CSP's infrastructure or supported missions.
- Protects DoD systems/applications instantiated in one CSP's infrastructure from incidents that affect a different CSP's infrastructure or supported missions.
- Extends the DoD demilitarized zone (DMZ) architecture via traffic segregation to externally (e.g., Internet) facing mission systems and applications in Level 4/5 CSOs. (i.e., implements a connection, physical or logical (e.g., MPLS VPN), between the CAP and the NIPRNet IAPs for Mission Owner applications providing their own application protections or leveraging an enterprise level application protection service provided by DISA or a DoD Component in the cloud. A CAP does not support/provide direct internet access to a Level 4/5 CSO. Such access must be via the IAPs
- May also terminate physical or logical connections from the internal side of a DoD Component's DMZ extension such that the DoD Component's existing DMZ/DMZ-extension protections may be leveraged).

The implementation of the DISN BCAP capability for NIPRNet is ultimately a DISA responsibility as part of its mission to protect the DoDIN and DoD information. Per the 15 December 2014 DoD CIO memo, initial capability may temporarily be provided by DoD Components other than DISA, as approved by the DoD CIO. This requirement is applicable to Boundary CAPs to the NIPRNet, not ICAPs. Specific CAP architectural requirements are beyond the scope of this SRG and will be published separately in the *Cloud Access Point Functional Requirements Document (FRD)*[76].

An ICAP capability for NIPRNet provides interconnection between CSP infrastructure at any impact Level 2-5 (dedicated to DoD) located inside the B/C/P/S "fence-line." (i.e., on-premises) The architecture of ICAPs may vary and may leverage existing capabilities such as the IA Stack protecting a DoD Data center today, JIE Core Data Center (CDC) tomorrow, or may be part of a Joint Regional Security Stack (JRSS). On the other hand, an ICAP may have special capabilities to support specific missions, CSP types (commercial or DoD), or specific cloud services. Since the CSP infrastructure and ICAP are both on-premises directly connected to the NIPRNet or indirectly via a DoD data center network, BCAP boundary protections are not needed. Alternate protections may apply. ICAP implementation and the connection of on-premises CSP infrastructure to the NIPRNet will follow normal NIPRNet connection approval guidance and requirements as is the case with any NIPRNet enclave or application infrastructure in a DoD data center.

Connection of a mission system to the DISN via an ICAP or BCAP will be approved and recorded by the DISA Connection Approval Office in accordance with normal connection approval procedures. This requires all Mission Owners to register all Cloud based applications, their CSP/CSO, and connection method in the DISA Systems/Network Approval Process (SNAP)[77] database Cloud Module. Initial connections (physical or virtual) to a CSP's network will occur during onboarding of the CSP's first Mission Owner customer. Additional connections will be made or capacity will be scaled as more Mission Owners use the given CSP.

[76] CAP FRD: http://iase.disa.mil/cloud_security/Pages/index.aspx (PKI required)
[77] SNAP: https://snap.dod.mil/gcap/home.do
Connection Approval: http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Approval

Specific processes and procedures regarding connection approval and Mission Owner connections via a BCAP are beyond the scope of this SRG and will be published separately.

Impact Level 2: Since off-premises CSP infrastructure having a Level 2 PA is directly connected to the Internet, all traffic to and from a Level 2 CSO serving Level 2 missions and their mission virtual networks will connect via the Internet. The NIPRNet BCAP is not used. See sections 5.10.2.2, *User/Data Plane Connectivity* and 5.10.2.3, *Management Plane Connectivity* for additional details.

Impact Levels 4/5: All DoD traffic from NIPRNet to and from off-premises CSP infrastructure serving Level 4 and level 5 missions and the mission virtual networks must traverse one or more NIPRNet BCAPs. No direct traffic is permitted to/from the Internet except via the NIPRNet IAPs and DoD DMZ capabilities provided by the Mission Owner, a DoD Component, or DISA. The BCAP terminates dedicated circuits and VPN connections originating within the CSP's network infrastructure and/or Mission Owner's virtual networks. This includes the production plane for non-privileged user access and the management plane for privileged user access and deployed IA/Cyber Defense tool connectivity to internal Cyber Defense monitoring systems. See Sections 5.10.2.2, *User/Data Plane Connectivity* and 5.10.2.3, *Management Plane Connectivity* for additional details. High availability Mission Owner systems and their supporting CSP network infrastructure must connect through two or more NIPRNet BCAPs. The NIPRNet BCAP will support Internet facing Mission Owner systems by minimally providing a physically or logically isolated path between the BCAP and the IAPs IAW the DMZ STIG. Some DMZ STIG capabilities/protections are the responsibility of the Mission Owner until such time as they are provided by the Mission Owner's agency or DISA as an enterprise service.

NOTICE: Level 5 CSP/CSO infrastructure/applications and DoD Mission Owner applications must be designed such that there is no dependence on Internet based resources such that traffic must traverse the IAPs to/from the Internet to make the CSO function. As such the CSO and DoD Mission Owner applications connected through a BCAP must be able to fully function, serving NIPRNet connected users in the event DoD decides to cut off NIPRNet access to the Internet. Of course in this situation, Internet connected users will not be able to utilize the Level 5 service/resource. Mission Owners that need this restriction for Level 4 CSOs must add the requirement to their SLA/contract.

NOTE: The Level 4/5 CAP connectivity requirements are intended for Mission Owner's systems migrating from on-premises DoD data centers on NIPRNet to a commercial CSO in an off-premises data center. Level 4/5 missions currently implemented and approved for having/utilizing direct internet connectivity (under DoD CIO waiver) (i.e., not internal to the DISN/NIPRNet behind the IAPs) are not required to utilize a NIPRNet BCAP as they migrate from physical infrastructure to the Cloud. However, such missions must use a CSO with a Level 4/5 PA and must minimally implement the same boundary protections as defined in this SRG for Level 2 missions due to being directly connected to the Internet.

Impact Level 6:

Since DoD on-premises Impact level 6 CSOs and their supporting infrastructure are required to be closed SIPRNet enclaves, they must comply with all SIPRNet connection approval requirements which include the appropriate enclave boundary protections and CDSP requirements. The DoD Mission Owner systems/applications instantiated in these Impact Level

6 CSO enclaves will be assessed and authorized the same way any other DoD SIPRNet enclave connection IAW the DISA Connection Process Guide. Approval for connection to the SIPRNet will be processed through the DISA classified connection approval process like any other SIPRNet enclave.

In accordance with CNSS architectural recommendations for the National Secret Fabric, DoD SECRET enclaves and virtual networks instantiated in DoD on-premises Impact level 6 CSOs will be considered as an enclave within the DoD provider network, (i.e., the SIPRNet). As such no SIPRNet BCAP is required for the connection of these DoD enclaves (physical or virtual) to the SIPRNet.

Corresponding Security Controls: SC-7, SC-7(3), SC-7(4)

5.10.1.1 Mission Partner Environments or Communities of Interest Network Cloud Access Points

For the purpose of this CC SRG, mission partner refers to DoD Components, Federal agencies, and potentially their contractors operating networks that include DoD and other entities. This section does not include or refer to war fighting coalition partners or the networks they use or are implemented for them. Coalition networks may be addressed in a future release of the CC SRG, however the use of cloud computing on these networks should be implemented in the same manner as this CC SRG provides for NIPRNet or SIPRNet depending on the classification level of the network.

Mission Partner Environments (MPEs) include mission partners that utilize networks other than NIPRNet or SIPRNet (e.g., DREN) and mission partner Communities of Interest (COI) that utilize network overlays and extensions that leverage (e.g., ride on or overlay) the NIPRNet or SIPRNet (e.g., MilCOI). Additionally, DoD Component mission partners (e.g., commissaries, exchanges, educational entities) typically operate networks that are not part of the DISN or .mil domain. These mission partners and their networks are typically in the .gov/.org/.com/.edu domains and may be directly accessed from the Internet through a boundary similar to a DoD IAP which they operate or a contracted third party DHS/GSA Trusted Internet Connection (TIC). Such other networks and COI may interconnect with NIPRNet or SIPRNet and may interconnect with other DoD and Non-DoD mission partner/Agency networks.

MPEs that utilize network(s) other than NIPRNet or SIPRNet (e.g., DRSN), will need to implement BCAPs or ICAPs for those network(s) that provide equivalent protections to those defined in the *CAP Functional Requirements* Document (FRD)[78] when connecting CSP infrastructure to their networks. MPEs implemented as a COI overlay on NIPRNet or SIPRNet can utilize the DISA-provided CAPs to fulfill the CAP requirement or may provide their own CAP capability IAW the CAP FRD. Mission Partners that are external to NIPRNet or SIPRNet, however, are responsible for providing an equivalent capability to protect DoD data and MPEs from vulnerabilities associated with a connection to an external service provider.

All MPE CAP instantiations must be approved by the DoD CIO.

[78] CAP FRD: Link to be added when published

5.10.2 Network Planes

A plane, in a networking context, is one of three integral components of network architectures. These three elements – the data synchronization/control or network plane, the user/data or production plane, and the management plane – can be thought of as different areas of operations. Each plane carries a different type of traffic and is conceptually an overlay network on top of the network plane.

5.10.2.1 Network Plane Connectivity

The network or data sync/control plane carries signaling traffic and data replication between servers/data centers. Network control packets originate from or are destined for a network transport device (virtual or physical). The network plane in general is subject to network related DoD SRGs and STIGs. This CC SRG does not contain additional requirements related to network plane connections to the cloud computing infrastructure.

5.10.2.2 User/Data Plane Connectivity

The user/data plane (also known as the forwarding plane, carrier plane, or bearer plane) carries the network user traffic. Table 5 details the DoD user/data plane connectivity by impact level for DoD on-premises and off-premises CSOs.

NOTE: While this table does apply to non-DoD Federal Government tenants using a DoD on-premises CSO, it does not apply to non-DoD Federal Government tenants using an off-premises CSO that is a Federal Government community cloud having DoD tenants.

Table 5 - User/Data Plane Connectivity

Impact Level	Off-Premises Non-DoD CSP Service Offering Infrastructure	On-Premises DoD and Non-DoD CSP Service Offering Infrastructure
Level 2	▪ User connectivity will leverage commercial infrastructure (i.e., Internet). ▪ Users connecting from the Internet will connect directly while users connecting from inside the DISN (i.e., NIPRNet) will connect to the Internet via the DISN Internet Access Points (IAPs) then to the CSP infrastructure. ▪ CSO connections will be assessed and authorized using the same external connection requirements as any other Internet-facing connection.	▪ User connectivity will use existing infrastructure (Government owned) for its user/data plane when the user is within the B/P/C/S fence-line (on-premises) and directly connected to the local Base Area Network (BAN) and NIPRNet. ▪ User traffic to/from the NIPRNet to/from the CSO infrastructure will traverse an ICAP. When the user is outside the B/P/C/S fence-line (off-premises) connected to the Internet, user traffic must enter/leave the NIPRNet via the DISN Internet Access Points (IAPs) then an ICAP via DoD DMZ extension. ▪ CSO connections will be assessed and authorized the same as any other
Level 4 And 5	▪ DoD and external user connectivity will leverage a DISN extension to the commercial facility using government network infrastructure within government boundaries (i.e.	

	NIPRNet) and commercial infrastructure beyond government boundaries (i.e. commercial carrier infrastructure / connectivity service offerings). ▪ The DISN extension will traverse a BCAP. ▪ Users connecting from inside the DISN (i.e., NIPRNet) will connect via a BCAP while users connecting from the Internet will traverse the IAPs then a BCAP via a DoD DMZ extension. ▪ CSO connections will be assessed and authorized through the Connection Approval Process the same as any other internal connection using the same requirements as any other DoD-facing or Internet-facing connection. Internet-facing connections are assessed and authorized IAW the DMZ STIG.	internal connection.
Level 6	▪ User connectivity will leverage a DISN extension to the commercial facility using government SECRET network infrastructure within government boundaries (i.e. SIPRNet) and commercial infrastructure beyond government boundaries (i.e. commercial carrier infrastructure / connectivity service offerings). ▪ The DISN extension to a commercial facility can be accomplished with a Multiprotocol Label Switching (MPLS) router and optical switch (referred to as a Service Delivery Node). ▪ The DISN extension to a commercial facility will use NSA Type 1 encryption or commercial equivalent (Commercial Solutions for Classified Programs (CSfC)[79] Suite B). ▪ User traffic to/from the Internet (e.g., executive travel kits users) will use	▪ User connectivity will use existing SECRET network infrastructure (Government owned) for its user/data plane (i.e., SIPRNet). User traffic to/from the SIPRNet will traverse an ICAP. ▪ User traffic to/from the Internet (e.g., executive travel kits users) will use NSA Type 1 encryption or commercial equivalent (CSfC Suite B) and must enter/leave the SIPRNet via the approved gateways. ▪ CSO connections will be assessed and authorized the same as any other internal connection using the same requirements as any other SIPRNet - facing connection (i.e., IAW the DMZ STIG).

[79] Commercial Solutions for Classified Programs: https://www.nsa.gov/ia/programs/csfc_program/index.shtml

	NSA Type 1 encryption or commercial equivalent (CSfC Suite B) and must enter/leave the SIPRNet via the approved gateways.	

5.10.2.3 Management Plane Connectivity

The management plane carries network/server/system privileged user (administrator) traffic along with maintenance and monitoring traffic.

Table 6 details the management plane connectivity by impact level for Mission Owner's systems/applications and CSP's CSOs. The Mission Owner management plane includes connectivity for DoD personnel or DoD contractors managing Mission Owner systems (i.e., virtual machines and networks) instantiated on IaaS/PaaS as well as for DoD personnel or DoD contractors access to / use of CSP service ordering/management portals for all service offering types (IaaS/PaaS/SaaS). The CSP management plane includes connectivity for CSP personnel managing the CSP's service offering infrastructure.

All encryption identified, except as stated otherwise, must be accomplished using FIPS 140-2 validated cryptography modules operated in FIPS mode.

IAW standard practice and security requirements, management interfaces on VMs and protective appliances (virtual or physical) located in a Mission Owner's virtual network, must not be exposed to direct access from the production network (e.g., Internet or NIPRNet/SIPRNet). To the extent possible, CSP service ordering/management portals through which VMs and virtual networks are instantiated and configured must also be protected from direct access from the production network to prevent compromise of mission systems and DoD information.

All management transactions must be audited.

Table 6 - Management Plane Connectivity

Impact Level	Mission Owner Management Plane	CSP Management Plane
Level 2	▪ **Management connectivity from outside the NIPRNet** (e.g., for off-premises contractor personnel) requires an encrypted, tunneled connection via the Internet to the mission system/application and virtual network. Management traffic to CSP service ordering / service management portals must be encrypted if not in an encrypted VPN. Monitoring traffic must traverse a VPN connection. All traffic entering/leaving the NIPRNet must be via the DISN Internet Access Points (IAPs).	▪ **Non-DoD CSP off-premises service offering infrastructure and off-premises management:** CSP management connectivity leverages CSP service offering and management plane infrastructure which should be logically or physically separate from production. NOTE: DoD cannot dictate how a CSP architects their commercial service offerings that are not dedicated to DoD. DoD recommends logical or physical separation of service offering production and management plane

	▪ **Management connectivity from inside the NIPRNet** (e.g., for on-premises DoD or contractor personnel) must be restricted to a defined set of IP addresses and requires an encrypted, tunneled connection through the NIPRNet to the Internet via the IAPs to manage the mission system/application and virtual network. Management traffic to CSP service ordering / service management portals must be encrypted if outside an encrypted VPN. Monitoring traffic must traverse a VPN connection. All traffic must enter/leave the NIPRNet via the DISN Internet Access Points (IAPs).	infrastructure as a well-known industry best practice. Such separation will be assessed as a bullet point for DoD risk acceptance. **Non-DoD CSP on-premises service offering infrastructure and management:** The CSP may directly connect their management infrastructure to their service offering infrastructure if collocated. An encrypted, tunneled connection from the CSP's on-premises management infrastructure to the service provider's on-premises service offering infrastructure is also permitted locally but must be used to access remote service offering infrastructure. ▪ **Non-DoD CSP on-premises service offering infrastructure and off-premises management:** CSP management connectivity must leverage an encrypted, tunneled connection from the CSP's off-premises management infrastructure to the service provider's on-premises service offering infrastructure. ▪ **DoD CSP on-premises service offering infrastructure and management:** CSP management connectivity will utilize existing infrastructure such as the Enterprise Services Directorate (ESD) Out of Band (OOB) management network. No service provider security stack is required.
Level 4 **And 5**	▪ **Management connectivity from inside the NIPRNet** must be restricted to a defined set of IP addresses and requires an encrypted, tunneled connection through the NIPRNet and an ICAP or BCAP to manage the mission system/application and virtual network. Management traffic to CSP service ordering / service management portals must be encrypted if not in an encrypted VPN. Monitoring traffic must traverse a VPN connection. All traffic must enter/leave the NIPRNet via a BCAP. ▪ **Management connectivity by DoD personnel or DoD contractors from outside the NIPRNet** must be restricted to a defined set of IP addresses and requires an encrypted, tunneled connection from the Internet via an IAP and an ICAP or BCAP to the mission system/application and virtual network. Per remote administration policy, the remote management terminal must be Government Furnished Equipment (GFE). Management traffic to CSP service ordering / service management	

	portals must be encrypted if outside an encrypted VPN. Monitoring traffic must traverse a VPN connection via a BCAP and NIPRNet.	
Level 6	▪ All management and monitoring connectivity is via the SIPRNet. Management and monitoring traffic will be encrypted using FIPS 140-2 validated cryptography[80] to accommodate separation for Need-to know reasons.	▪ **DoD CSP on-premises service offering infrastructure and management:** CSP management connectivity will utilize existing SECRET network infrastructure such as the SECRET Out of Band (OOB) management network. No service provider security stack is required. ▪ **Non-DoD CSP on-premises service offering infrastructure and management:** The CSP may directly connect their management infrastructure to their service offering infrastructure if personnel are collocated using their SECRET LAN. An encrypted, tunneled connection using FIPS 140-2 validated cryptography over SIPRNet from the CSP's on-premises management infrastructure to the service provider's on-premises service offering infrastructure is also permitted and will be used to access remote service offering infrastructure. ▪ **Non-DoD CSP on-premises service offering infrastructure and off-premises management:** CSP management connectivity must leverage a SIPRNet extension or a DoD approved encrypted, tunneled connection from the CSP's dedicated SECRET off-premises management infrastructure to the service provider's on-premises service offering infrastructure. ▪ **Non-DoD CSP off-premises service offering infrastructure and off-premises management:** CSP

[80] FIPS 140-2 validated cryptography: http://csrc.nist.gov/groups/STM/cmvp/index.html

		management connectivity leverages CSP's dedicated SECRET service offering and management plane infrastructure which must be logically or physically separate.

5.10.3 CSP Service Architecture

DoD uses the concept of defense-in-depth when protecting its networks and data/information. This includes, but is not limited to, hardening host OSs and applications, implementing host firewalls and intrusion detection, strong access control, robust auditing of events, while protecting the networks with application layer firewalls, proxies, web content filters, email gateways, intrusion detection / prevention, and a DMZ /gateway architecture, along with robust network traffic monitoring. The concept must not be lost when moving Mission Owners systems/applications and their data/information to the commercial cloud. As such, if virtualization is used, the above measures must also be used to protect the virtual environment along with the use of hypervisor based firewall/filtering/routing mechanisms or virtual security appliances.

This section details the defense-in-depth security concepts and requirements that both CSPs and Mission Owners must implement to protect DoD data/information and mission systems/applications. DoD recognizes that there are innovative approaches that can be implemented in the virtual environment that may replace some of the defense-in-depth mitigations that have been developed over the years for physical networks and servers. DoD looks forward to evaluating equivalent alternative measures which will be assessed by DISA on a case by case basis.

5.10.3.1 CSP Service Architecture - SaaS

Mission Owner use of CSP's SaaS offerings are reliant on the defense-in-depth measures implemented by the CSP for the protection of the service application and the infrastructure that supports it. This includes the protection of all sensitive information stored and processed in the CSP infrastructure. In other words, the Mission Owner relies on the CSP and the security posture of its SaaS offering for the protection of DoD information. During the ATO assessment process for SaaS offerings, defense-in-depth security / protective measures must be assessed for adequacy and potential risk acceptance by DoD. This may be in addition to assessing security controls. The following guidance is reflected in the DoD DMZ STIG and Application Security and Development STIG along with other operating system (OS) and application specific STIGs, but is highlighted here to emphasize instances where an authoritative reference (e.g., product specific STIG) is not available.

The defense-in-depth security / protective measures to be established by the CSP for SaaS are, but are not limited, to the following:

- Application Layer Firewall (properly configured) and intrusion detection and/or prevention protection of the CSP's infrastructure supporting the SaaS application

offering, as well as segmentation (logical or physical) from the CSP's other offerings and corporate networks.

- Application / network architecture which provides unrestricted/restricted DMZ zones with appropriate protections IAW the DoD DMZ STIG for internet/externally facing servers and private / "back end" zones with appropriate protections for application/database servers and other supporting systems/servers. This includes but is not limited to Web Application Firewalls, Reverse Web Proxies, FTP Proxies, etc. as necessary for the protection of the application and the customer's data/information stored/processed within.
- Customer data-at-rest encryption protections using FIPS 140-2 validated cryptographic modules operated in FIPS mode where only the Mission Owner has control of the keys. This requirement addresses the persistent storage of customer data on various media and in databases, not customer data that requires real time processing without retention. If such data is retained then the retained data storage is persistent.
- Customer data-in-transit encryption protections using FIPS 140-2 validated cryptographic modules operated in FIPS mode. This requirement addresses customer data transiting public and private Wide Area Networks (WAN) (i.e., Internet, NIPRNet, CSP's WAN) and Local Area Networks (LANs) from the customer terminal to the CSP's service offering enclave LAN. Encryption may be native at the protocol level or be at the VPN/tunnel level. This requirement is also applicable to CSP replication of customer data and systems between primary locations and backup Continuity of Operations (COOP) / Disaster Recovery (DR) locations.
- Hardening / patching / maintenance of OSs and applications IAW industry standards. DoD SRGs and STIGS or DoD-accepted equivalents must be used if the service is private or community cloud used by DoD. For Information Assurance (IA) Vulnerability Management (IAVM) message compliance, the CSP will be expected to comply with industry best practice by applying patches identified in the CVE that would be referenced in the DoD IAVM message. Innovative alternatives such as implementing a behavioral based or software integrity protection model for all systems may be viable and will be assessed on a case by case basis.
- Implement PIV/DoD CAC / PKI authentication for all customer user access on all SaaS offerings that process information at impact Levels 4 and 5 in accordance with IA-2 (12). This includes regular non-privileged users accessing the service and privileged customer users accessing service ordering / management interfaces/portals. SaaS offerings that process information at impact Level 6 must use the CNSS SIPRNet Token. Alternate authentication measures for those user communities that cannot use the required PKI token will be assessed on a case by case basis and may require a waiver.

NOTE: Equivalencies to the vulnerability mitigations provided in DoD SRGs and STIGS may be viable and acceptable but must be approved by the DISA AO.

NOTE: IAVM messages include IA Vulnerability Alerts (IAVA), IA Vulnerability Bulletins (IAVB), and Technical Advisories (TA). For the remainder of this SRG, the term IAVMs will be used to refer to all IAVM message types.

5.10.3.2 CSP Service Architecture - IaaS/PaaS

Mission Owners build systems and applications on virtualized infrastructure provided by the CSO under IaaS/PaaS. There must be a clear delineation of responsibility for security between the CSP and the Mission Owner, which depends on how the CSP presents the security features it supports in the CSO. Under IaaS the Mission Owner is fully responsible for securing the guest operating systems and applications that they build; the CSP will be responsible for securing the virtualization OS (i.e., hypervisor) and supporting infrastructure. Under PaaS, the Mission Owner is fully responsible for securing the guest operating systems and the platform applications and applications that they build. Depending upon how the CSP CSO presents the security features it supports in the CSO, the delineation of responsibility may partially shift from the Mission Owner to the CSP with respect to the guest operating systems and the platform applications. The CSP might take responsibility for securing these areas of a PaaS CSO as part of the core service or as an add-on component.

For the purpose of the remainder of Section 5 of this SRG, IaaS and PaaS offerings are generally treated the same with the responsibility of securing the OS and platform applications being that of the Mission Owner. Mission Owners must assess inherited mitigations that the CSP provides to determine that defense-in-depth security / protective requirements are fully met.

CSP IaaS and PaaS offerings must support the defense-in-depth security / protective measures that the Mission Owner must implement to secure the systems and applications that they build on the service offering. These measures are defined in Section 5.10.6, *Mission Owner System/Application Requirements using IaaS/PaaS*.

5.10.3.3 CSP Disaster Recovery (DR) - Continuity of Operations (COOP)

As a best business practice, CSPs plan for Disaster Recovery (DR) and Continuity of Operations (COOP) and implement their infrastructures to support it. This typically includes geographically separate facilities/data centers. Furthermore, FedRAMP assess several C/CE related to Contingency Planning (i.e., DR and COOP).

Data replication between CSP geographically separate facilities/data centers is typically required for Disaster Recovery (DR) and/or Continuity of Operations (COOP) which includes backup.

All Data replication must traverse a CSP's private internal network (physical or virtual) from CSP offering site/location to the DR/COOP facility and protect the data in transit. If this network traverses the Internet, the network connection must be encrypted end-to-end in an IPsec tunnel implemented using FIPS 140-2 validated cryptography. Separation requirements implemented in the CSO between DoD data and non-DoD data at the CSP offering site/location must be replicated at the DR/COOP facility. Such separation is not specifically required in transit unless its implementation is required to support separation at the endpoint facilities.

NOTE: For Level 4/5 CSOs such transfers do not route through the DISN BCAP unless the DR/COOP facility is on-premises or is another CSP's CSO.

Related Controls: CP-6, CP-7, CP-9

5.10.4 Internet Protocol (IP) Addressing and Domain Name Services (DNS)

DoDI 8410.01, *Internet Domain Name Use and Approval*, 4 December, 2015[81] provides DoD policy on the use of Top Level Domain (TLD) names by DoD organizations, their ISs and networks.

DoDI 8410.01 requires DoD to conduct DoD public and private Internet-based communications (e.g., electronic mail and Web operations) under the TLD established for the DoD—the *.mil* TLD". Exceptions are provided for some DoD organizations which may use the .gov, .edu, and .com domains if necessary and approved by the Mission Owner's CIO. This means that the end user accessing a DoD web site or other resource using a URL will see ".mil" at the end of the URL (e.g., name.mil is required vs name.com).

DoDI 8410.01 additionally requires DoD to only use the .mil domain to provide names for IP addresses allocated or assigned to the DoD by the American Registry for Internet Numbers (ARIN) and specifically states that these IPs are to be assigned in accordance with the DoD NIC Registry Protocol 9802. DoD NIC Registry Protocol 9802 then goes on to state that

> a. ... IP address space is assigned by the DoD NIC for use on a DoD common user data network and may not be used to obtain access to the Internet via a commercial Internet Service Provider.
>
> And
>
> b. IP address space will only be used on the common user network to which it is registered. IP address space or subnets of IP address space will not be shared amongst different common user networks. For example, IP address space assigned for SIPRNET use must be used only on the SIPRNET while IP address space assigned for NIPRNET use must be used only on the NIPRNET.

Interpret this to mean that DoD IP addresses are to only be used on DoD systems located on registered DoD networks.

Furthermore it requires that a .mil URL not redirect to non-.mil domain named hosts (e.g., name.mil will not redirect to name.com) with the only exception being for an approved and accredited service that provides redirection not readily apparent to the end user (e.g., use of a content delivery service or cloud service). This exception permits the use of a Canonical Name (CNAME) in the system's DNS record within the DoD DNS servers that redirects the URL to the CSP assigned URL associated with the commercial IP address. As such the end user must not be made readily aware of the redirection.

NOTE: The example of electronic mail (email) in DoDI 8410.01 paragraph 3.a and previously in this section does not negate the use of an external commercial cloud email service by DoD Components providing the URL to access the service ends in ".mil" and the redirection is not readily apparent to the user.

NOTE: IP addresses assigned by ARIN to the DoD NIC which are then assigned to DoD Components for their networks and information systems (e.g., NIPRNet addresses) are unique publicly routable addresses. Only within DoD enclaves are "private" (non-publicly routable) RFC 1918 addresses permitted/used.

[81] DoDI 8410.01: http://www.dtic.mil/whs/directives/corres/pdf/841001p.pdf

5.10.4.1 IP Addressing

Off-Premises Impact Level 2:

Due to off-premises Impact Level 2 IaaS/PaaS/SaaS CSOs being directly accessed from the Internet, DoD Mission Owner systems/applications using the .mil domain that are implemented in an Impact Level 2 IaaS, PaaS, or SaaS CSO will be addressed using public IP addresses assigned and managed by the CSP. This also applies to DoD Mission Owner systems/applications approved to use non-.mil domain names. In this case the DoD DNS server will use a CNAME to point to the commercial URL and its IP address.

NOTE: The use of "private" RFC 1918 IP addresses internal to the virtual network enclave with commercial addresses on the Internet facing interfaces is acceptable and is recommended minimally for topology hiding.

Off-Premises Impact Level 4/5:

DoD IP addresses are assigned/managed by the DoD Network Information Center (NIC) and may be further managed and assigned to networks and ISs by DoD component NICs. In accordance with DoD policy NIPRNet, subtended Component enclave networks, and their internally connected endpoints are addressed using DoD NIPRNet IP addresses.

NOTE: The following is NOT applicable to DoD systems that are not connected to, or not part of, the NIPRNet and are already approved to use Non-DoD, Non-NIPRNet, IP addresses. There is no intent to force such DoD systems to become part of the NIPRNet.

Since, by default, Mission Owners systems/applications instantiated in IaaS and in some PaaS CSOs have full control over the IP addressing of their systems/applications instantiated in the CSO, and since they are connected to NIPRNet through a NIPRNet BCAP, DoD NIPRNet IP addresses will be used. This also applies to SaaS where the Mission Owner has control over the IP addressing used in their portion of the CSO. As such these systems/applications are within a network enclave that is considered an extension of the NIPRNet. The DoD NIC has set aside a range of NIPRNet IP addresses for CSOs connected to the NIPRNet BCAP. This requirement applies similarly to networks other than NIPRNet where a BCAP is required. In such cases IP addresses used on that network will be used.

NOTE: As with any DoD enclave, The use of "private" RFC 1918 IP addresses internal to the virtual network enclave with NIPRNet addresses on the NIPRNet/Internet facing interfaces connected via the CAP is acceptable.

DoD recognizes that with some off-premises commercial SaaS and some PaaS CSOs today, the Mission Owner may not have control over the IP addressing of the CSO and CSP managed IP addresses must be used and interfaced with the NIPRNet via the BCAP. The preferred solution is for the CSP to provide a NAT or proxy between the CSO and NIPRNet BCAP. Alternately the routing of CSP managed commercial IP addresses must be segregated from other routing and traffic on the NIPRNet by using a Multiprotocol Label Switching (MPLS) VPN or similar method. Since such a solution is not scalable for all Mission Owner's to have their own MPLS VPN, such VPNs will be shared. CSP managed IP addresses used for DoD missions must be dedicated to DoD and must not be accessible from the Internet. This is in support of DoD Cyber Defense, network routing, and the prevention of unauthorized access and back doors.

NOTE: DoD's objective requirement for all off-premises Level 4/5 CSP's CSOs serving the DoD is for the CSO to offer a "bring your own" IP address capability for all customer facing interfaces so that DoD NIPRNet IP addresses may be used. In this case, customer facing interfaces includes general user interfaces and customer management interfaces including customer service management/ordering portals. This IP addressing request does not include CSP systems instantiated within the CSO infrastructure that are not directly accessible from the NIPRNet (or other mission partner network) which may use CSP assigned and managed IP addresses.

Off-premises Impact Level 6:

All off-premises CSP's Level 6 CSOs will be treated, designed, and addressed as an extension of the SIPRNet (i.e., a SIPRNet enclave) or other SECRET mission partner network.

All Mission Owner systems/applications instantiated in IaaS/PaaS (i.e., VMs and virtual network device interfaces) and connected to SIPRNet will be addressed using SIPRNet IP addresses. This includes management plane systems and interfaces.

All off-premises CSP Level 6 SaaS and some PaaS service offerings connected to SIPRNet must utilize DoD assigned and managed SIPRNet IP addresses throughout. Alternate addressing will require a waiver.

On-premises Impact Level 2/4/5:

All on-premises Level 2/4/5 IaaS/PaaS/SaaS CSOs and Mission Owner systems/applications will be addressed using DoD NIPRNet IP addresses.

On-premises Impact Level 6:

All on-premises Level 6 IaaS/PaaS/SaaS CSOs and Mission Owner systems/applications will be addressed using DoD SIPRNet IP addresses.

5.10.4.2 Domain Name Services (DNS)

DoD .mil DNS servers on NIPRNet (and .smil.mil DNS servers on SIPRNet) are authoritative for DoD IP addresses provided through the DoD NIC and subtended Component NICs. This means that the DoD .mil DNS servers resolve .mil URLs to their destination IP address. DoD .mil DNS servers on NIPRNet must also be used to host .mil URLs which cannot have a specific IP address associated with it. In this case, a CNAME is used in the DoD .mil DNS servers on NIPRNet to point to a commercial URL used by the CSO.

DoD .mil DNS servers on NIPRNet are protected using various security measures such as the DoD DNS proxies, the Enterprise Recursive service, and DNSSec. As such DoD DNS is protected from many DNS threats and DoD DNS and associated protective services must be used for DoD .mil URLs and address resolution as appropriate.

General Rule, All On-Premises and Off-Premises Impact Levels 2/4/5:

In general and IAW DoDI 8410.01 Mission Owner systems/applications using the .mil domain instantiated in an IaaS/PaaS/SaaS CSO where the Mission Owner has control over the IP addressing and is using DoD NIPRNet IP addresses, must host their .mil DNS records in the DoD .mil NIPRNet authoritative DNS servers, not public or commercial DNS servers.

Therefore, such Mission Owners are not authorized to utilize DNS services offered by the CSP or any other non-DoD DNS provider unless otherwise approved to use another domain.

NOTE: Mission Owners using non-.mil URLs may utilize CSP managed or other commercial/public DNS servers (not the DoD DNS servers) for the domains in which they are authorized to operate.

The following exceptions to the general rule noted above apply:

Exception for Off-Premises Impact Level 2:

DoD Mission Owners using an off-Premises Impact Level 2 CSO which by default uses CSP managed commercial IP addresses and URLs must host their .mil DNS records in the DoD .mil NIPRNet DNS servers and use a CNAME to point to the commercial URL or IP address as appropriate. CSP DNS servers will be authoritative for commercial IP address resolution.

Exception for Off-Premises Impact Levels 4/5 SaaS and some PaaS:

DoD Mission Owners using an off-premises Impact Level 4/5 CSO (IaaS and some PaaS) where the Mission Owner does not have control over the IP addressing and therefore is dependent upon CSP managed commercial IP addresses and URLs must host their .mil DNS records in the DoD .mil NIPRNet DNS servers and use a CNAME to point to the commercial URL for IP address resolution as appropriate. CSP DNS servers will be authoritative for their commercial IP address resolution.

In the event their use is required CSP DNS services including URL redirection and dynamic DNS solutions along with implemented DNS protections will be assessed and approved as appropriate for the CSO's DoD PA. CSP DNS services must be protected using a DNS proxy and must support DNSSec. The DoD PA will also include a risk assessment of the CSP's DNS management architecture or outsourced services.

All On-Premises and Off-Premises Impact Level 6:

DoD Mission Owners using an on-premises or off-premises Impact Level 6 CSO will use smil.mil URLs whose DNS records will be hosted on the DoD authoritative DNS servers on the SIPRNet (or other SECRET mission partner network). SIPRNet addresses are assigned by the DoD NIC.

Corresponding Security Controls: SC-20, SC-21, SC-22

5.10.5 Mission Owner Requirements using SaaS (All Levels)

While protecting/securing/defending the SaaS architecture is the responsibility of the CSP, Mission Owners contracting for and using CSP's SaaS offerings must minimally address the following to meet DoD policy:

- Register the Protocols and Services along with their related UDP/TCP IP Ports used by the SaaS service that will traverse the DISN in the DoD PPSM registry. This includes all user and management plane traffic for Levels 4, 5, and 6 as well as management plane traffic for Level 2 if managed/monitored from within a DoD network. See Section 5.15, *Ports, Protocols, Services, Management and Cloud* for additional information.
- Register the service/application with the DoD whitelist for both inbound and outbound traffic if traffic will cross the IAPs.

Register the CSP's CSO in the DISA SNAP database for the connection approval which also includes the designation of a certified CDSP as the Mission Cyber Defense (MCD) as defined in Section 6, *Cyber Defense and Incident Response.*

This step is required at all levels for SaaS, including level 2 (even though there is no production connection to the DISN) so that the DoD CDSP community is aware and informed such that they can perform their Cyber Defense duties described in Section 5.18, Supply Chain Risk Management Assessment.

As discussed in Section 5.10.3, *CSP Service Architecture*, the Mission Owner is reliant on the security posture of the CSP and their SaaS offering for the protection of DoD data/information.

5.10.6 Mission Owner System/Application Requirements using IaaS/PaaS

Mission Owners must address defense-in-depth security / protective measures across all information impact levels when implementing systems/applications on IaaS / PaaS which include, but are not limited to, the following:

- Implement Virtual Machines (VMs) in one or more virtual networks in which data-flows between VMs and between VMs and external networks (both physical and virtual) may be controlled.
  NOTE: Virtual networks are typically a feature of the virtualization hypervisor which supports the VMs.
- Implement virtual 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 a tiered architecture with 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.
- In the event the mission system/application is internet facing, implement (in addition to a zoned architecture described above) DMZ protections IAW the DMZ STIG. For example the DMZ STIG requires the following (adapted for Cloud):
  - Web server in a public virtual network zone
  - Application and database servers in a private virtual network zone
  - Two Routers (virtual for cloud):
    - Outer – public zone to Internet
    - Inner public zone to private zone
  - Reverse Web Proxy (RWP)
  - FTP proxy if FTP is used
  - Web Application Firewall (WAF)
  - Security Information Manager (SIM)
  - Syslog server
  - Two Active directory servers
    - Public zone
    - Private zone

  Impact Level 2: DMZ boundary protection requirements (i.e., proxies and firewalls) must be implemented by the mission owner for their application(s) or leverage a common boundary service provided by a larger entity like DoD Component or the DoD enterprise.

This will most likely occur on a CSP by CSP basis. Other common services may also be available.

Impact Level 4: DMZ boundary protection requirements (i.e., proxies, firewalls, etc.) will be provided by the Mission Owner in their system/application environment until such time as these protections are provided by the Mission Owner's agency or DISA as an enterprise service.

- When infrastructure has direct Internet access, implement virtual application level firewall and virtual intrusion detection and/or prevention capabilities IAW the applicable DoD SRGs and STIGs to protect the virtual network(s) and interconnected VMs. The Mission Owner and/or their CDSP must be able to control firewall rules and monitor the virtual network boundary, reporting same to the Tier 1. For dedicated infrastructure with a DISN connection (Levels 4-5): implement firewall, IPS, and/or routing methods that restrict traffic flow inbound and outbound to/from the virtual network to the DISN connection IAW DoDI 8551. Block all traffic from all other sources such as the CSP's network which is most likely connected to the Internet.
- Implement a secure (encrypted) connection or path (i.e., encrypted VPN) between the virtual firewall, the virtual IDS capabilities and the CDSP responsible for the mission system/application. See Section 6, Cyber Defense and Incident Response. for more specific information.
- IaaS: Securely configure (harden / STIG) / patch / maintain each VM's OS and IAW DoD policy and CYBERCOM direction. The use of DoD STIGs and SRGs is required for secure configuration as is compliance with IAVMs.
- PaaS: For those VM OSs and applications under direct management of the Mission Owner (not the CSP per contract), securely configure (harden /STIG) / patch / maintain each VM's OS and application provided by the CSP IAW DoD policy and United States Cyber Command (USCYBERCOM) direction. The use of DoD STIGs and SRGs is required for secure configuration as is compliance with IAVMs.
- IaaS/PaaS: Securely configure (harden / STIG) / patch / maintain each application provided/installed by the Mission Owner IAW DoD policy and USCYBERCOM direction. The use of DoD STIGs and SRGs is required for secure configuration as is compliance with IAVMs.
- Implement data-at-rest encryption on all DoD files housed in CSP IaaS storage service offerings. A CSP may offer one or more services or methods to accomplish this. Data-at-rest encryption may help mitigate issues with data/information spillage. See Section 5.11, *Encryption of Data-at-Rest* for more information
- If the DoD information is sensitive government information (e.g., FOUO or CUI), FIPS 140-2 validated software cryptography modules operated in FIPS mode must be used.
- All encryption services for data-at-rest must be implemented such that the Mission Owner has sole control over key management and use.
- Implement Host Based Security System (HBSS) IAW DoD policy.
  - Implement HBSS agents on all VMs with a supported general purpose OS.
  - Utilize an HBSS agent control server within NIPRNet.
  - Implement a secure (encrypted) connection or path (i.e., encrypted VPN) between the HBSS agents and their control server.
  - Provide visibility by the Mission Owner's CDSP entities as defined in Section 6, Cyber Defense and Incident Response.

- Implement scanning using an Assured Compliance Assessment Solution (ACAS) server IAW USCYBERCOM TASKORD 13-670.
  - Implement a secure (encrypted) connection or path (i.e., encrypted VPN) between the ACAS server and its assigned ACAS Security Center.
- Provide visibility by the Mission Owner's CDSP entities as defined in Section 6, Cyber Defense and Incident Response.
  - Implement DoD PKI server certificates for establishing secure connections.
- Implement all required data-in-transit encryption protections using FIPS 140-2 validated cryptography modules operated in FIPS mode.
- Implement DoD CAC / PKI authentication as follows:
  - For all privileged user access to VM operating systems and applications for Levels 2, 4, and 5 IAW DoD policy. Level 6 must use the CNSS SIPRNet Token.
  - For all general DoD users of the implemented systems/applications for Levels 4 and 5 IAW DoD policy. Level 6 must use the CNSS SIPRNet Token.
  - Implement a secure (encrypted) connection or path (i.e., encrypted VPN) between the implemented systems/applications and the DoD OCSP responders on NIPRNet or SIPRNet as applicable
- Secure 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 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. See Section 5.10.7, *Active Directory Integration for Cloud* for more information.
- Register the Protocols and Services along with their related UDP/TCP IP Ports used by the Mission Owner's system/service/application that will traverse the DISN. This includes all traffic for Levels 4, 5, and 6 as well as management/monitoring plane traffic for Level 2. See Section 5.15, *Ports, Protocols, Services, Management and Cloud* for additional information.
- Register the Mission Owner's system/service/application with the DoD whitelist for both inbound and outbound traffic if traffic will cross the IAPs.
- Register the Mission Owner's system/service/application and CSP's CSO in the DISA SNAP database for the connection approval which also includes designating a certified CDSP as the Tier 2 MCD. This step is required at all levels for IaaS/PaaS, including level 2 (even though there is no production connection to the DISN) so that the DoD CDSP community is aware and informed such that they can perform their Cyber Defense duties described in Section 6, *Cyber Defense and Incident Response*.
- Implement Computer Network Defense and Incident Response for monitoring issues across all CSPs used by DoD.

NOTE: Under PaaS (and potentially IaaS) where CSPs may be under contract to securely configure (harden / STIG) / patch / maintain Mission Owner's VMs, OSs, applications, or maintain STIGed and patched VM images for their use, such services must be validated to DoD standards IAW all applicable policies (e.g., privileged access). If the CSP is contracted by the Mission Owner to securely configure OSs and applications, then the CSP is expected to comply with all applicable DoD STIGs. For IAVA compliance, the CSP will be expected to comply with industry best practice by applying patches identified in the CVE that would be referenced in the DoD IAVA. Equivalencies will be assessed and approved on a case by case basis.

5.10.7 Active Directory Integration for Cloud

Active Directory (AD) implementations (if needed) will be configured IAW the Active Directory Domain and Forest STIGs[82] along with the following guidance related to Cloud services:

- DoD/Commercial CSP CSO on premises private/community (e.g., milCloud) managed AD:
  - AD servers and forests may establish trust relationships with other DoD managed AD servers and forests IAW established DoD guidelines.
- DoD Mission Owner managed AD instantiated in DoD/Commercial CSP CSO on premises private/community IaaS/PaaS (e.g., milCloud):
  - AD servers and forests may establish trust relationships with other DoD managed AD servers and forests IAW established DoD guidelines.
- DoD Mission Owner managed AD instantiated in Commercial off-premises IaaS/PaaS:
  - DoD AD forests will not trust Mission Owner managed AD servers or forests instantiated in Commercial IaaS/PaaS.
  - AD servers and forests may trust other DoD managed AD servers and forests IAW established DoD guidelines. This trust must be one way. Alternate methods than a direct trust such as those described in the following subsections should be used.
    NOTE: this mitigates the potential for a compromised Mission Owner's AD in the commercial CSO being able to compromise a DoD AD on the DISN
- Non-DoD CSP CSO managed AD:
  - A Non-DoD CSP's AD may be used to provide access control services to the CSO if it is an integral part of the CSO. (e.g., for SaaS)
  - DoD AD forests will not trust a Non-DoD CSP's AD servers or forest.
  - Only if absolutely required, a Non-DoD CSP's AD forest may trust a DoD AD forest. This trust must be one way. Alternate methods than a direct trust such as those described in the following subsections should be used.
    NOTE: this mitigates the potential for a compromised CSP's AD being able to compromise a DoD AD on the DISN.

NOTE: Established DoD guidelines for AD implementation are found in the AD Domain and Forrest STIGs noted above.

5.10.7.1 Active Directory Federation Services (ADFS)

Active Directory Federation Services (ADFS) is used to extend on-premises Active Directory access control credential use and single sign-on (SSO) capabilities to web servers located in another organization such as a CSP's SaaS CSO. This capability will enable access control to multiple web applications over the life of a single browser session. This is also applicable to providing SSO capabilities to a mission owner's own web application instantiated in IaaS/PaaS CSO without placing an AD server in the virtual environment. Since ADFS in essence allows the CSP's CSO or external web application to trust the DoD identity claim asserted on behalf of the DoD AD, the use of ADFS meets the intent of the AD requirements stated above.

[82] Active Directory Domain and Forest STIGs: http://iase.disa.mil/stigs/os/windows/Pages/active-directory.aspx

5.10.7.2 Active Directory DirSync (Directory Synchronization)

Active Directory DirSync is a Microsoft Azure tool which is specific to a specific Microsoft SaaS CSO. DirSync is installed on a domain-joined server (on-premises or on a Microsoft Azure VM) to "synchronize your on-premises Active Directory users to Office 365 for professionals and small businesses"[83]. Since this tool provides user information to the Office 365 AD as a push, then the Office 365 AD is used to provide access control to the CSO for those users, this tool meets the intent of the Non-DoD CSP managed AD requirements stated above.

5.11 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 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 utilize encryption hardware/software on the DISN or a cloud encryption service that provides DoD control of keys and key management.

Data-at-rest (DAR) encryption with customer controlled keys and key management protects the DoD data stored in CSOs with the following benefits:

- Maintains the integrity of publicly released information and web sites at Level 2 where confidentiality is not an issue.
- Maintains the confidentiality and integrity of CUI at levels 4 and 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 trough increasing the work necessary to compromise/access unencrypted DoD data.
  - Enables high-assurance data destruction for CSP off-boarding through cryptographic erasure and file deletion without the involvement or cooperation of a CSP.
  - Enables high-assurance data spill remediation through cryptographic erasure and file deletion without the involvement or cooperation of a CSP.
  - See Section 5.11.1, *Cryptographic Erase* for additional information.

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

For all Information Impact levels:

- Encrypt all Data at Rest (DAR):
  - Stored in virtual machine virtual hard drives or
  - Stored in mass storage facilities/services whether at the block or file level
  - Stored in database records (whether PaaS, SaaS where the MO does not have sole control over the DB and DBMS)

[83] DirSync: https://technet.microsoft.com/en-us/library/dn635310.aspx

- Using FIPS 140-2 validated cryptography modules[84] (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 Customer / Mission Owner (MO) 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 customer/MO

For cloud applications where encrypting DAR 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 take into account that there may be no high-assurance method available to remediate data spills or ensure destruction of data at the application's end of life and CSO off-boarding. Mission Owner AOs are responsible for accepting these risks.

NOTE: CSPs CSOs DAR encryption capabilities and ability to support Mission Owner's DAR encryption requirements will be assessed and documented toward the award of their DoD PA.

Corresponding Security Controls: SC-28, SC-28(1)

5.11.1 Cryptographic Erase

Cryptographic erase is described in NIST SP 800-88 Rev 1[85]:

"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 itself. CE techniques are typically capable of sanitizing media very quickly and could support partial sanitization, a technique where a subset of storage media is sanitization. Partial sanitization, sometimes referred to as selective sanitization, has potential applications in cloud computing."

While much of the CE guidance in SP 800-88 is related to self-encrypting devices, this section expands on NIST's acknowledgement that CE has applicability in cloud computing.

DAR encryption, coupled with exclusive customer control of cryptographic key management, provides DoD the ability to cryptographically erase data at rest without CSP assistance or cooperation. This capability coupled with standard CSP provided data deletion provides the following benefits described for DAR encryption in Section 5.11 above.

Data deletion refers to normal file or data record deletion methods used in file systems and data bases. Deletion before or after cryptographic erase will restore resources to the CSP and will permit for the eventual overwriting of the data under normal operations.

[84] NIST FIPS CMVP: http://csrc.nist.gov/groups/STM/index.html http://csrc.nist.gov/groups/STM/cmvp/index.html
[85] NIST SP 800-88: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

To support cryptographic erase and the various benefits it provides DAR 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)

5.12 Backup

CSPs are responsible for providing backups of data in a CSO consistent with the CP-9 security control. Mission Owners are also responsible for assuring their data is backed up consistent with the CP-9. However, mission owners must also consider the risk of entrusting their data to a single non-DoD CSP. Section 5.8, *Data Retrieval and Destruction for Off-boarding from a CSO* discusses the importance of Mission Owners being ready to recover and/or migrate their data on short notice in case of CSO shutdown. This readiness, along with CSP backup requirements, may be sufficient for DoD data of low to moderate impact value. However, Mission Owners with higher impact value data should consider conducting regular backups of their data and storing them in DoD-owned infrastructure/media or a cloud storage service offered by a different CSP.

Backups stored with a different provider reduce the risk of data loss/corruption in the case of a CSO ceasing operations or catastrophic event that affects a CSP's entire infrastructure. Maintenance of such backups may also mitigate the risk of data loss sustained from of a data spillage response. Mission Owners should determine the potential need for such risk mitigation as part of the contingency planning required by the CP-2 security control.

NOTE: In the case of IaaS/PaaS backups, "data" as used in this section includes VM snapshots or images of the fully configured VMs including their virtual hard drives so that restoration of the computational base is as easy as the restoration of the information processed.

NOTE: This section is provided for consideration by Mission Owners. It does not affect CSPs or DoD PA assessments.

Corresponding Security Controls: CP-2, CP-9

5.13 DoD Contractor / DoD Component Mission Partner Use of CSOs

This section focuses specifically on Non-CSP DoD contractors or mission partners (e.g., Defense Industrial Base (DIB) contractors) and DoD Component mission partners (e.g., commissaries, exchanges, educational entities) whose networks that are not part of the DoDIN .mil domain. These mission partners and their networks are typically in the .gov, .org, .com, .edu domains.

When using cloud services, mission partners and contractors are responsible for following all guidance in this CC SRG related to the Mission Owner that is not specific to a DISN-provided capability (e.g. CAP) or an enterprise service. The appropriate impact level must be selected based on the DoD data being processed. A trusted means of communication that encrypts all DoD data transferred between mission partners and contractor internal networks and CSPs must be utilized. Mission partners and contractors are also responsible for working with the appropriate DoD data owner or designated agency (e.g. DSS) to create incident response procedures for incidents that occur in a CSO.

NOTE: the term "Non-CSP DoD Contractors" as used below does not include DoD Contractors that are not a CSP but aggregate CSOs (i.e., integrators) in the fulfilment of a contract for cloud

services. As such, and as noted elsewhere in this CC SRG, the CSOs these non-CSP integrators are providing via subcontracts must follow all guidance related to CSOs and DoD's usage of them.

5.13.1 DoD Component mission partners

DoD Component mission partners in the .gov, .org, .com, .edu domains must only use CSPs or CSOs that have a DoD PA for the Information Impact Level that best matches the CNSSI 1253 categorization of the information to be processed/stored/transmitted by the CSP/CSO. If the information is public, then a Level 2 CSO will be used with direct Internet access. Otherwise, accessing Level 4/5 services depends on how their organizational network/enclave is connected today. This is as follows:

- The organizational network/enclave: Is part of NIPRNet; connectivity to the CSO will be via the NIPRNet BCAP
- Is part of a Mission partner or CIO network with a BCAP; connectivity to the CSO will be via that BCAP
- Is directly connected to the Internet via one or more approved organizational IAPs; connectivity to the CSO will be via the Internet or a private direct connection

DoD Component mission partners are responsible for implementing appropriate boundary protections for their networks.

5.13.2 Non-CSP DoD Contractors and DIB Partners Use of CSOs for the Protection of Sensitive DoD Information

Non-CSP DoD contractors and DIB partners may store, process, and use or create sensitive DoD data/information outside of the DoDIN in conjunction with a DoD contract not associated with providing cloud services. Such contractors are required to protect unclassified sensitive DoD data/information while it is in their environment IAW DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*[86] and NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*[87] which mainly focuses primarily on confidentiality.

Non-CSP DoD contractors and DIB partners may wish to utilize Cloud Services in the fulfilment of their contract or for the protection/processing of DoD data they possess. Thus, for the protection of sensitive DoD information, it is highly recommended that Non-CSP DoD contractors utilize CSOs that have been granted a DoD Level 4/5 PA that best matches the CNSSI 1253 categorization of the information to be processed/stored/transmitted by the CSP/CSO. Such CSOs must not be dedicated to DoD which would mean the CSO is only connected to the NIPRNet. That said, access to the CSP/CSO will be via the Internet or a private direct connection. The NIPRNet will not be used as a connection path. DoD contractors are responsible for implementing appropriate boundary protections for their networks.

[86] DoDI 8582.01: http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf
[87] NIST SP 800-171: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

5.13.3 Non-CSP DoD Contractors Use of CSOs as a Portion of a Non-CSO Product or Service

A Non-CSP DoD Contractor might choose to integrate a third party CSO as a component of a contracted Non-CSO product or service (e.g., a weapons system or major application). Such contractors may only utilize third party CSPs or CSOs that have a DoD PA for the Information Impact Level that best matches the CNSSI 1253 categorization of the information to be processed/stored/transmitted by the CSP/CSO. Furthermore, the CSO and its use must follow the CC SRG guidance related to the Mission Owner that is not specific to a DISN-provided capability (e.g. CAP) or an enterprise service to the greatest extent possible. Connectivity to the CSO will be determined by where the contracted product or service will be used and related guidance in this CC SRG. For example if the user base for the product or service is NIPRNet based and the Information Impact Level is 4 or 5, then the NIPRNet BCAP must be used. If the Information Impact Level is 2, then the Internet may be used. All CC SRG requirements apply to the product and flow down to the sub-contracted CSO IAW various DFARS clauses.

In the event the Non-CSP DoD contractor chooses to provide/host the CSO themselves, the CC SRG requirements for the Information Impact Level that best matches the CNSSI 1253 categorization of the information to be processed/stored/transmitted by the CSO applies. If the CSO is dedicated to the product, A&A will handled IAW normal DoD contract A&A requirements. Consideration for awarding a DoD PA in this case will depend on the results of the A&A processes, compliance with the CC SRG, and the potential for other DoD Component's Mission Owners to use the CSO.

5.14 Mission Owner DoD Test and Development in the Cloud

Cloud environments are a good place Mission Owners to do application development and testing as well as research. Furthermore, test and development activities associated with application lifecycle management for cloud based applications are best performed in the same environment as the production application. This section addresses DoD Test and Development (T&D) activities in IaaS and PaaS CSOs.

Security requirements for DoD T&D and laboratory environments are defined in the suite of Enclave T&D STIGs[88]. Refer to these STIGs on IASE for the latest guidance.

The Enclave T&D STIG Overview document defines four (4) T&D Zones. These zones are briefly described as follows:

- Zone A: Instrumental in application lifecycle management for final end stage testing prior to implementation into a production environment. This environment is connected to the production network to replicate the final production environment supporting the application. The use of VPNs for remote access for developers and administrators may be implemented, but must be terminated in the T&D DMZ for inspection. The assets in the environment are secured the same as the production environment to include STIG and IAVM compliance. Minimal development is permitted for final revisions and minor updates in the final testing phase.

[88] T&D STIGs: http://iase.disa.mil/stigs/net_perimeter/enclave-dmzs/Pages/index.aspx

- Zone B: Instrumental in application lifecycle management for application development activities such as coding, compliance, and testing. This environment provides connectivity to the production network with access controls in place to protect the production network for application testing. Provides an isolated network segment for the use of tools and capabilities to facilitate application development that would not be permitted in the production environment. Implements remote access to the testing segment of the environment for developers and administrators. Is secured WRT STIG and IAVA compliance at the discretion of the IAM.
- Zone C: Closed test environment not connected to DoD production networks but interconnects multiple testing environments through the use of direct connections or tunneling mechanisms. This environment can be used for testing systems, devices, applications, tools, and/or protocols where their security posture or potential to threaten DoD production networks is unknown or known to be risky while needing long-haul network connectivity.
- Zone D: A fully closed and physically separate network from any DoD live operational network for the purpose of extensive testing using prohibited tools, working with malicious code, virus samples, working with Ports, Protocols, and Services (PPS) that are otherwise restricted via DoD policy. Development within this environment is generally not an encouraged practice.

All DoD test and development performed in cloud infrastructure must be categorized IAW the T&D Zone descriptions in the Enclave T&D STIG Overview document and comply with the security requirements in the associated Enclave T&D STIG.

Since Zones A and B are instrumental in application lifecycle management and able to be connected to the production network, it is reasonable that these zones can be implemented in the same IaaS/PaaS cloud infrastructure as the production applications they support. Due to the robust routing and filtering capabilities inherent in today's virtual networks, the segmentation of these zones can easily be implemented IAW the related Zone A and B STIG requirements using VLANs or distinct virtual networks.

DoD application development Zone B instantiated in cloud infrastructure must minimally be implemented in a CSP's CSO that has a Level 2 PA. Consideration for implementing Zone B in a Level 4/5 CSO will depend on the sensitivity of the application itself and its code. If the Zone B is used for the lifecycle management of a production application, then it should be implemented in the same CSP/CSO as the production application.

DoD application test Zone A instantiated in cloud infrastructure must be implemented in the same CSP/CSO as the production application to support lifecycle management of the application. The sensitivity of the information processed by the production application determines the information impact level of the CSP and their PA IAW this SRG, thus the test environment using similar data must be at the same information impact level.

It is highly recommended to realize the efficiencies of the Cloud that Zones A and B be implemented in the same CSO and impact level where the final production application will operate in support of its lifecycle management and ease of migrating the application from Zone B through Zone A to production. As such, access to these zones will be via the same path (i.e., Internet or DISN BCAP) as is used for the production zone with the exception that access to zone B will use the management plane only.

While Zones C and D are typically implemented in physical facilities and while various aspects may use virtualization, these zones may only be implemented in cloud services providing the required lack of connectivity to DoD production networks. This generally precludes on-premises cloud services which are intended for wide usage by multiple DoD tenants such as milCloud as designed today. Alternately Zones C and/or D might be implemented in an off-premises commercial cloud environment where there is no direct connectivity to DoD networks, providing the testing activities do not threaten the CSP's CSO and/or network, other CSP tenants' systems/applications or the Internet. Exceptions and requirements for these use cases may be provided in a future release of this or another SRG. Zones C and D which might be categorized at Levels 4/5/6 and implemented in off-premises CSOs are not permitted to connect to the DISN.

Corresponding Security Controls: CM-4, CM-4 (1)

5.15 Ports, Protocols, Services, Management and Cloud Based Systems/Applications

Mission Owners using CSOs of any service type (I/P/SaaS) must comply with DoDI 8551.01: *Ports, Protocols, and Services Management (PPSM)*[89] when implementing and operating their systems/applications in an IaaS/PaaS CSO or when using a SaaS offering. DoDI 8551.01 is the DoD policy that provides policy guidance for DoD Mission Owner compliance with CM-7, CM-7 (1), and SA-9 (2). While CSPs must comply with these C/CE for their internal networks and service offerings, DoDI 8551.01 does not apply to CSPs as the policy applies to Protocols And Services (PS) traversing the DISN.

The DISA PPSM office[90] [91], along with the PPSM Change Control Board (CCB) and Technical Advisory Group (TAG) publish a Category Assignment List (CAL) which lists the PS permitted to cross certain DISN boundaries and Vulnerability Assessments (VAs) for each PS listed. Compliance with VAs is the key to the secure usage of the PS listed in the CAL. In other words, PS used on the DISN must comply with the associated VA. Mission Owners must utilize the mitigations presented in the PPS VAs when building their systems. Additionally all Mission Owners must register their cloud CSO based systems/applications in the DoD PPSM Registry (only available on SIPRNet) to include systems/applications in an I/PaaS CSO or when using a SaaS offering. Registration includes all PS along with their related UDP/TCP IP Ports used by the application that will traverse the DISN. This includes all user and management plane traffic for Levels 4, 5, and 6 as well as management plane traffic for Level 2 if managed/monitored from within a DoD network.

The remainder of this section of the CC SRG provides guidance to mission owners when registering their applications in the PPSM database.

Level 2 Off-premises CSO: A Level 2 Mission Owner virtual network, virtual machines, and applications in IaaS/PaaS CSOs constitute a DoD enclave within and accessed via an external network. Similarly a SaaS CSO is an enclave within and accessed via an external network. This external network is the Internet. So for Level 2 the Mission Owner should leverage PPSM guidance for PPSM boundaries 1-5. This is only applicable to Mission Owner's management traffic for their virtual networks and systems/applications in IaaS/PaaS and CSO management

[89] DoDI 8551.01: http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf
[90] PPSM Office IASE page: http://iase.disa.mil/ppsm/Pages/index.aspx
[91] PPSM Office Public page: http://disa.mil/network-services/Enterprise-Connections/PPSM

traffic for I/P/SaaS. When registering the application in the PPSM database the Mission Owner should register on boundaries 1-5. Since non-privileged user traffic will be via the Internet, registration is not required even if a portion of this traffic is to/from non-privileged users within the DoDIN. Such traffic will traverse the DISN IAPs as any other web based traffic.

NOTE: This guidance may change with regard to user plane traffic pending a decision of the PPSM CCB. Since firewalls and sensors are required at the boundary of a Mission Owner's virtual enclave and since the sensors will be monitored by the MCD protecting the Mission Owner's system/application, the same or similar guidance as is provided for Level 4/5/6 below may be applicable.

Level 2/4/5/6 On-premises CSO: On-premises CSOs at any level will be treated as normal DoD enclaves. PPSM Registrations will utilize boundary designations 7-11 if directly connected or 10-12 and 15 if connected via an IPSEC tunnel.

Levels 4/5/6 Off-premises CSO: IAW the CC SRG, Levels 4/5/6 Off-premises CSOs will be treated as normal DoD enclaves since they are architected as extensions of the DoDIN/DISN even though the CSO is in an external network (the CSP's network) and are connected via a BCAP. As such, PPSM Registrations will utilize boundary designations 7-11 if directly connected or 10-12 and 15 if connected via an IPSEC tunnel.

NOTE: PS designated as local services may be used within the Mission Owner's system/application virtual enclave in IaaS/PaaS CSOs as with any other enclave providing they do not traverse the virtual enclave's boundary.

5.16 Mobile Code

Mobile code is defined as software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc.

Mobile Code presents a great number of attack vectors to both CSPs and DoD Mission Owners. CSP organizational IT systems as well as the infrastructure that supports CSOs are vulnerable to malicious mobile code, and if compromised, the security of DoD Mission Owner's systems/applications/information/data can be negatively affected. Additionally compromised CSOs and DoD Mission Owner's systems/applications can negatively affect a customer's endpoint and network if malicious mobile code is served by (downloaded from) these systems.

While DoD mobile code policies are under revision, CNSS and DoD has identified mobile code in categories as follows:

> "Category 1: Mobile code technologies that exhibit a broad functionality, allowing unmediated access to the workstation, server, and remote system services and resources. Category 1 mobile code technologies have and pose known security vulnerabilities with few or no countermeasures once executing.
>
> Category 2: Mobile code technologies that have full functionality, allowing mediated access to the workstation, server, and remote system services and resources. Category 2 mobile code technologies have and pose known security vulnerabilities, however, known fine grained, periodic, or continuous countermeasures/safeguards exist.

Category 3: Mobile code technologies that have limited functionality, with no capability for unmediated access to the workstation, server, and remote system services and resources. Category 3 mobile code technologies may have a history of having and posing known security vulnerabilities, but also support known fine grained, periodic, or continuous countermeasures/safeguards.

Emerging Mobile Code Technologies: All mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and been categorized as described above."

While most of the compliance with DoD Mobile Code policy is the responsibility of the Mission Owner, SC-18 (2) states "The organization ensures that the acquisition, development, and use of mobile code to be deployed in information systems meets organization-defined mobile code requirements". The following applies to DoD IS:

"(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.

(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.

(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).

(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used."

DoD expects the CSP to enact similar Mobile Code Policies for SC-18 (2) for their organizational IT systems and the infrastructure supporting their CSO(s) for the protection of the CSO(s), Mission Owners' systems/applications/information/data in the CSO. Furthermore DoD expects that the CSP's CSO will not enable or permit the download of unapproved/risky mobile code, for the protection of the CSO's end users as well as Mission Owner's and their end user's systems and networks. SC-18 (2) is under consideration for addition to the FedRAMP+ baseline for all impact levels.

Similarly SC-18 (3) and SC-18 (4) have been assigned values in Table 9. These are currently in the set of SLA controls to be considered by Mission Owners for inclusion in the SLA/Contract. These too, are under consideration for addition to the FedRAMP+ baseline for all impact levels.

Mission Owners systems/applications must not download and execute mobile code except as permitted above, and must not enable or permit the download of unapproved/risky mobile code, for the protection of the system's/application's end users as well as their end user's systems and networks.

5.17 Registration and Connection Approval for Cloud Based Systems/Applications

This section provides information on the various registrations required for cloud based systems/applications in addition to PPSM registration discussed in Section 5.15, *Ports, Protocols, Services, Management and Cloud Based Systems/Applications*.

5.17.1 DISA Systems/Network Approval Process (SNAP)

All Mission Owners are required to register all Cloud based systems/applications; their CSP/CSO, MCD, and connection method in the DISA Systems/Network Approval Process (SNAP)[92] database Cloud Module. This registration will enable these systems/applications to be connected to the DISN and is crucial for the situational awareness of the Cyber Defense community tasked with protecting the DoDIN, DoD information, and the Mission Owners Cloud based systems/applications.

5.17.2 DoD Whitelist

In the event the Mission Owners Cloud based systems/applications requires traffic to traverse the DISN IAPs, the systems/applications URLs/IP addresses must be registered with the DoD DMZ Whitelist. Traffic that will typically traverse the IAP is management traffic for Level 2 off-premises systems/applications and for user plane traffic to/from Level 4/5 systems/applications that are internet facing (i.e., accessed from the Internet via the DoD DMZ extension connected to a BCAP). Such traffic and IP addresses may be blocked if not registered in the Whitelist. Mission Owners must contact their DoD Component's point of contact to have their entry added to the Whitelist.

5.17.3 Select and Native Programming Data Input System- Information Technology (SNaP-IT)

In compliance with the DoD Memo, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," 15 Dec 2014, DoD Components will report all appropriate information within the Select and Native Programming Data Input System-Information Technology (SNaP-IT)[93] as directed in DoD CIO annual IT budget guidance for each utilized cloud computing service. SNaP-IT is the authoritative DoD database used for publishing the DoD IT Budget estimates to Congress and the OMB Circular A-11 Section 53 and Section 300 exhibits to OMB for Information Technology. To comply, Components MUST respond to the SNaP-IT Profile questions for the Exhibit 53 into two submissions; the Exhibit 53A, 'Agency IT Investment Portfolio Summary', and the Exhibit 53C, the 'Agency Cloud Computing Spending Summary'. Components must identify whether a cloud computing option was evaluated for each investment, and provide detail as instructed. Components fulfill their requirement for all Exhibits 53s by completing their SNaP-IT Profile, Resource, and Budget Support Data for each component investment.

5.18 Supply Chain Risk Management Assessment

The DoD selected FedRAMP+ control SA-12 addresses Supply Chain Risk Management (SCRM) while SA-19 deals with component authenticity. The acquisition of system components and software that are counterfeit, unreliable, or contain malicious logic or code is of great concern to DoD for all products supporting the processing, storage, and transmission of CUI and classified information. This concern extends to Cloud Computing.

---

[92] SNAP: https://snap.dod.mil/gcap/home.do
Connection Approval: http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Approval

[93] SNaP-IT U: https://snap.pae.osd.mil/snapit/loginauth.aspx for Levels 2/4/5 systems/applications
SNaP-IT S: https://snap.cape.osd.smil.mil/snapit for Level 6 systems/applications

As part of the CSO's DoD PA assessment package, the CSP will provide a SCRM plan outlining their supply chain assessment/management and component authenticity process and measures taken such that they are not acquiring system components and software that are counterfeit, unreliable, or contain malicious logic or code and incorporating them into the CSO infrastructure or its management plane.

The CSP's SCRM plan for how the CSP implements SA-12 and SA-19 will be assessed and approved during the DoD PA assessment process for all Impact Level 4, 5, and 6 CSOs.

5.19 Electronic Mail Protections IAW TASKORD 12-0920

US CYBERCOM Task Order (TASKORD) 12-0920 requires the use of the Enterprise E-Mail Security Gateway (EEMSG) for all email inbound from, or outbound to, the Internet. It further requires email outbound from one DoD Component's email servers to another Component's email servers to pass through the EEMSG. The EEMSG only deals with server to server email traffic, it does not deal with client to server traffic. All DoD Components are required to use the EEMSG unless a waiver is in place. In the event a waiver is in place, the DoD Component must use their own email security gateway.

Therefore IAW the full TASKORD:

- All email transfers inbound through the IAP from an external email server destined to a L4/5 email server in a Mission Owner's enclave within a CSO via a BCAP must pass through the EEMSG inbound protections.
- All email transfers sent from a L4/5 email server in a Mission Owner's enclave within a CSO via a BCAP and through the IAP to an external email server must pass through the EEMSG outbound protections
- All email transfers sent from a L4/5 email server in a Mission Owner's enclave within a CSO via a BCAP to email servers in a DoD Component's data center enclave must pass through the EEMSG outbound protections.
- All Email transfers sent from email servers in DoD Component's data center enclave to a L4/5 email server in a Mission Owner's enclave within a CSO via a BCAP must pass through the EEMSG outbound protections.

This requirement and interpretation of the TASKORD is based on the fact that the Mission Owner's environment in any CSO is considered a DoD enclave that may include an email server either as the primary service SaaS offering or as an adjunct service to a PaaS/SaaS, or may be instantiated by the Mission Owner in IaaS.

In the event two Mission Owners utilize the same email SaaS and email servers, there is no need for EEMSG protections for email between the different Mission Owners' users. However, in the event the CSO implements different servers/enclaves for different Mission Owners, the CSO must include an email hygiene/protective service through which email transfers between these servers/enclaves will route. In this case the server-to-server email traffic will remain within the CSP's infrastructure and not traverse the CAP or EEMSG. Similarly, Mission Owners that implement email servers in IaaS or leverage a PaaS feature within their CSO based enclaves will follow the same rules as above for SaaS and must provide for email hygiene/protective service within the CSO for enclave to Mission Owner enclave to Mission Owner enclave traffic or route such traffic through the BCAP and EEMSG.

All BCAPs must support Mission Owner's and implement the appropriate routing of server-to-server email traffic to/from the EEMSG capability at the CAP end of the connection for all CSOs that contain an email server. This includes routing to/from such servers and the IAP for email servers that are external and Internet connected. This is a CSO connection approval requirement. However it is ultimately a Mission Owner responsibility for TASKORD compliance when they use a CSO or implement a system/application in IaaS/PaaS.

NOTE: As of this release of the CC SRG, EEMSG does not currently inspect intra-enclave email. Therefore the above requirements do not apply to email traffic that remains within the DISN and Mission Owner enclaves in a CSO, until EEMSG does inspect intra-enclave email. That said, the requirement for EEMSG to inspect all email traffic to/from the Internet based email servers still applies.

This page is intentionally blank.

6 CYBER DEFENSE AND INCIDENT RESPONSE

Cyber Defense addresses the defense and protection of networks and Information Systems (ISs), detection of threats, and response to incidents. Cyber Situational Awareness (CSA) improves the quality and timeliness of collaborative decision-making regarding the employment, protection, and defense of DoD systems and data. The DoD Cyber Defense Command and Control (C2) structure provides the means to react to threats and incidents to defend the DoDIN. These are among the key challenges in DoD's adoption of Cloud Service Offerings (CSOs). This section addresses critical Cyber Defense requirements; tiers, roles and responsibilities; incident reporting and response; and other Cyber Defense processes.

6.1 Overview of Cyber Defense Tiers

DoD operates a tiered Cyber Defense C2 structure as defined in DoDI O-8530.2, *Support to Computer Network Defense (CND)* soon to be replaced by DRAFT DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations". The structure consists of United States Cyber Command (USCYBERCOM) and Joint Forces Headquarters DoDIN (JFHQ-DoDIN) at the top tier (Tier 1) and a network of Cyber Defense Service Providers (CDSPs) (Tier 2) that have been accredited by USCYBERCOM IAW DoD policy. Each DoD information system is operated/managed by a Mission Owner (Tier 3) which must be aligned with an accredited CDSP (Tier 2) which monitors and protects the information systems and associated assets. The Mission Owner is responsible for the implementation and maintenance of the security posture of their system(s) in accordance with SRGs/STIGs, and DoD policy in coordination with, and/or with the assistance of their aligned CDSP. CDSPs report information to USCYBERCOM which maintains Cyber Situational Awareness over all DoD networks and ISs. USCYBERCOM also provides threat information collected from various sources and threat mitigation orders to the CDSPs and Mission Owners.

NOTE: An example of maintaining the security posture of a Mission Owner's system is the application of patches/upgrades and IAVM compliance. This is a Tier 3 function or responsibility. While some DoD Components (e.g., Army) relieve their Mission Owners of some, or all, security posture maintenance activities by transferring their performance to the system's CDSP (e.g., ARCYBER), they remain Tier 3 functions and responsibilities. As such, the Tier 2 CDSP is responsible for performing the transferred Tier 3 functions along with their Tier 2 functions.

NOTE: The DoD Cyber Defense policy, processes, and lexicon. The CC SRG reflects those processes and has been updated to the . in this release of the CC SRG has been coordinated with the new Cyber Defense lexicon defined in DRAFT DoDI 8530.01 and DoD Joint Publication 3-12 (R), "Cyberspace Operations"

6.2 Concept Changes for Tiers for Cloud Computing

With the move to commercial cloud computing, the DoD is adopting a risk-based approach in applying network defense capabilities and processes. As described in Section 3.2, *Information Impact Levels.* DoD has defined Information Impact Levels commensurate to the risk and type of data, with each higher level warranting greater protections.

With Impact Level 2 data, the overall value of the data is not mission critical or sensitive in nature, thus it may not warrant the same level of protections as higher impact level data, while still needing protection. Recognizing that the data at Impact Level 2 has minimal requirements for confidentiality, emphasis must be placed on integrity and availability that achieve a level of security and risk acceptable to the responsible AO. User connectivity to the information system flows through the CSP's Internet connection; thus DoD is relying on the network boundary protections and monitoring available through the CSO if any. If the boundary defense is not implemented by the CSP, then the mission owner will be responsible and must coordinate with their DoD CDSP. Protection capabilities supporting the mission system at the system/host/application level will be provided by a combination of the CDSP and the mission system administrators (including the CSP for SaaS).

Level 4 and above data presents greater risk and thus necessitates the need for enterprise defense mechanisms and data collection that enable robust monitoring, event correlation, and analytics. With level 4 and above data, the DISN 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 through a few different entities: the CSP through monitoring of their CSO (especially for SaaS); the mission administrators or owners; or the CDSPs that are 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 Cyber Defense C2 structure, including the identification of entities with new Tier 2 Cyber Defense Command and Control (C2) and Operations (Ops) responsibilities. The use of a BCAP drives the requirement for two distinct functions/roles: Boundary Cyber Defense and Mission Cyber Defense.

6.2.1 Boundary Cyber Defense

Boundary Cyber Defense (BCD) monitors and defends the connections to/from CSPs via an authorized BCAP. BCD guards against the risk that each CSP interconnection poses to the DoDIN individually, along with cross-CSP analysis for all connections flowing through an individual BCAP. While this function focuses on the connections through a particular BCAP, cross-CAP analysis is warranted to determine if a threat extends beyond a single CSP or BCAP.

All anomalies identified by a BCD will be forwarded to DISA for cross-CAP analysis activities. The DISA Command Center (DCC) and DISA NetOps Center (DNC) Continental US (CONUS) are assigned global Cyber Defense C2 and Ops responsibility for protecting the DoDIN. This C2 construct addresses potential impacts across the multiple missions supported by a CSP, ensuring that Mission Owners and supporting MCDs have access to global situational awareness.

6.2.2 Mission Cyber Defense

Mission Cyber Defense (MCD) provides services to a Mission Owner's cloud-based mission systems/applications and virtual networks. Any given MCD may service cloud-based mission systems/applications and virtual networks instantiated in multiple CSPs and multiple CSOs. MCD is not a new Tier 2 entity; rather it is the integration of existing DoD CDSPs with a focus on elements of cloud computing. The MCD will typically be the CDSP used by the Mission Owner's Command, Service, or Agency (CSA) for their non-cloud-based ISs; however, Mission Owners can choose to use and fund any certified CDSP for their MCD provider.

6.3 Cyber Defense Roles and Responsibilities

The following is a list of the CND C2 functional elements and their responsibilities as it relates to cloud operations.

- **DoDIN/DISN Cyber Defense:** A Tier 1 function of the DCC and DNC CONUS focused on cross-DoDIN risk in DoD's use of cloud computing and commercial CSPs.
  - Responsible for protecting the DoDIN and DoD mission systems in commercial cloud infrastructure through cross-CAP correlation and analysis of events/data.
  - Directs or recommends C2 actions regarding DoDIN-wide incident and system health reporting involving a BCAP or CSP; elevates C2 recommendations to JFHQ-DoDIN as needed for cross-CSP/CSO incident response.
  - For DoDIN-wide incidents, establish and maintain external communications with the CSP and ensure internal DoD communications are established between all entities which include the MCD and BCD.
  - Interfaces with US-CERT to obtain relevant CSP information; ensures cross-sharing of information across all BCD/MCD entities.
- **Boundary Cyber Defense (BCD):** A Tier 1 and Tier 2 function of a certified Cyber Defense provider responsible for the management and monitoring of a BCAP.
  - Responsible for protecting the DoDIN and DoD mission systems in commercial cloud infrastructure connected via the BCAP.
  - Coordinates communications between USCYBERCOM / JFHQ-DoDIN and MCDs providing MCDs timely access to BCD-collected indications and warnings relevant to MCD subscribers.
  - Responsible for monitoring CSP adherence to incident response processes and advising the CSPs via the respective MCD on protecting their infrastructure and the DoD mission systems that they host.
- **Mission Cyber Defense (MCD):** Tier 2 responsibilities integrated in the existing DoD CDSPs focused on cloud computing. At a minimum, the MCD is responsible for:
  - Monitoring, protecting, and defending the Mission Owner's cloud-based systems, applications, and virtual networks in the CSP's IaaS/PaaS infrastructure.
  - Monitoring, protecting, and defending the Mission Owner's cloud-based data in the CSP's IaaS/PaaS infrastructure and Impact Level 4/5/6 SaaS infrastructure.
  - Analyzing cyber incidents and events for their subscriber Mission Owners.
  - Ensuring internal DoD communications are established between all entities which include the Mission Owner, MCD, and BCD.
  - Providing information on CSPs and missions being supported and the supporting BCD to DoDIN Cyber Defense and the JFHQ-DoDIN for situational awareness.
- **Mission Administrators:** Administrators of Mission Owner's cloud-based systems, applications, and virtual networks; a Tier 3 entity, at a minimum consuming CDSP services, is responsible for:
  - Following Tier 1 and Tier 2 direction.
  - Maintaining and patching the cloud-based mission systems, applications, and virtual networks.
  - Installing and maintaining protective measures for the cloud-based mission systems, applications, and virtual networks.
    NOTE: As noted in Section 6.1, *Overview of Cyber Defense* Tiers some DoD Components might transfer some or all of these responsibilities to the MCD.

- **The CSP:** CSPs provide for their own Cyber Defense services to provide for a secure environment for their customer's (DoD Mission Owner's) systems, applications, and virtual networks. In effect, the CSP will function as an extension of the DoD Cyber Defense Tier 3 entity (i.e., the Mission Owner) toward this end. At a minimum, CSPs are responsible for:
  - Providing local operational direction and support for Cyber Defense within their infrastructure and service offerings.
  - Fully maintaining, patching, monitoring, and protecting the infrastructure, operating systems, and applications supporting all service offerings.
  - Fully maintaining, patching, monitoring, and protecting the portions of PaaS service offering OSs and applications for which they are responsible (which may vary from none to all) as defined in the service offering SLA/description and/or the Mission Owner's SLA/contract..
  - Fully maintaining, patching, monitoring, and protecting SaaS service offering OSs and applications including DoD data/information in them.
  - And as contracted:
    - Coordinating with the MCD regarding incident response and the mitigation of threats to DoD cloud based mission systems/applications and data.
    - Providing timely incident and system health reports.
    - Maintaining bidirectional Cyber Situational Awareness.
  - Additional CSP responsibilities as may be defined in the Cloud Cyber Defense Concept of Operations (CONOPS) document published alongside the CC SRG.
- **Mission Owners:** Individuals/organizations responsible for the overall mission environment, ensuring that the functional and Cyber Defense requirements of the system are being met. At a minimum, Mission Owners are responsible for:
  - Engaging and funding the services of a MCD to provide for the defense of the Mission Owner's systems, applications, and virtual networks in any CSP's IaaS/PaaS infrastructure (whether DoD operated or operated by a commercial/non-DoD entity).
  - Establishing the terms and requirements in the contract with the CSP for incident reporting, incident response, and communications with the appropriate MCD and BCD providers.

Figure 10 and Figure 11 provide a graphic representation of these entities and the flow of communications between them.

Figure 10 depicts the Cloud Cyber Defense C2 model. JFHQ-DODIN has direct tasking authority over DCD, BCDs, and MCDs. JFHQ-DODIN, as part of USCYBERCOM, has legal authority to collaborate with entities external of DoD, such as the United States Computer Emergency Readiness Team (US-CERT). The Mission Owners, as the CSO subscribers to the CSPs, are the default C2 relationship to the CSPs. Mission Owners can optionally expand Cyber Defense-relevant reporting to their selected MCDs and BCDs by including such language in their Service Level Agreements (SLAs).

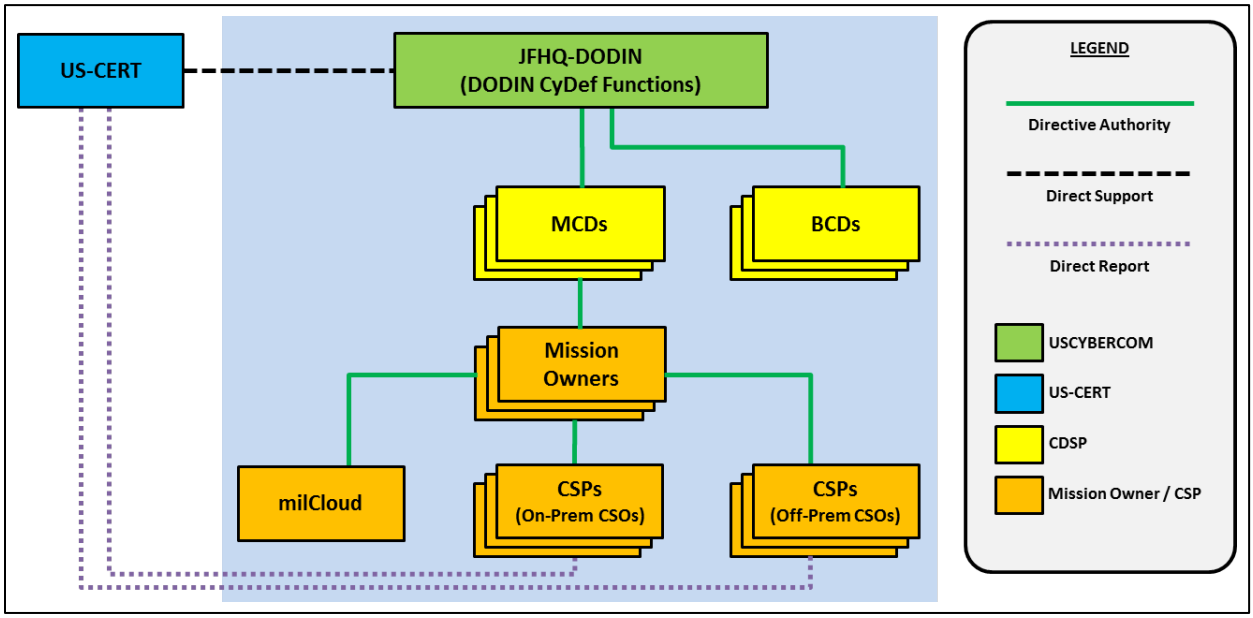

Figure 10 - DoD Cloud Incident Response and Cyber Defense C2 Model

To support JFHQ-DODIN, DCD performs Cross-Cloud Analysis (XCA) to enable "populate once and reuse many", enabled by the Cyber Defense Data Sharing (see Figure 11). Given that a single CSP may provide multiple and simultaneous service offerings for different Mission Owners, for each CSP, DCD will analyze potential impacts across the multiple missions, CSOs, and CSPs based on information coming from the MCDs.

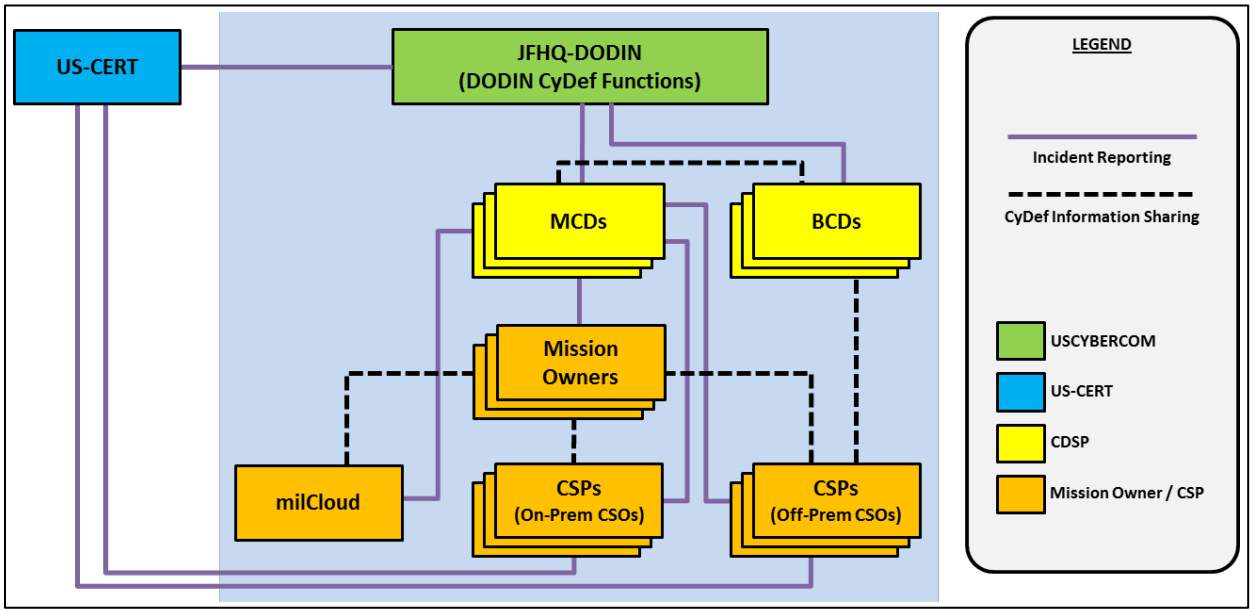

Figure 11 – DoD Cloud Incident Response and Cyber Defense C3 Data Sharing

The Cloud Cyber Defense C3 data sharing structure builds a comprehensive cyber SA picture across the MCDs, BCDs, DCD, JFHQ-DODIN and the CSPs. Incident and event data is correlated at the DCD and JFHQ-DODIN to minimize duplication of effort, minimize miscommunication (e.g. different descriptions for "same" incident spanning multiple CSOs), improve responsiveness and enable greater proactive defense for the Mission Owners across all of the CSOs.

6.4 Cyber Incident Reporting and Response

Two key definitions related to this section as reflected in the CNSSI 4009, IA Glossary, are as follows:

cyber incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident.
incident	An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

For the purposes of this SRG, we will use incident and cyber incident interchangeably.

FedRAMP, through the selection and implementation of IR-6, requires CSPs to report cyber incidents to the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team[94] (US-CERT) and the consuming Federal Agencies. For CSOs that are multi-tenant or otherwise shared across Federal Agencies outside of the DoD (Impact Levels 2 through 5), incidents will be reported to US-CERT as required by FedRAMP, in parallel with reporting to DoD. For CSPs providing dedicated infrastructure to the DoD (Impact Levels 4 and above), incidents regarding that infrastructure and CSOs will not be reported to US-CERT, but directly to the DoD. The DoD Tier 1 (USCYBERCOM/JFHQ-DoDIN) will handle coordination with US-CERT and other entities as appropriate. The DoD incident reporting process is described in Section 6.4.3, *Incident Reporting Mechanism.*

All CSPs actively supporting DoD missions will be supported by one or more MCD. The MCD(s) will be the DoD point of contact to which the CSP's Operational entity will coordinate response to incidents affecting the security posture of the CSP and the CSP's cloud service offerings. The MCD will coordinate with the higher tiered BCD as appropriate.

Corresponding Security Controls: IR-4, IR-5, IR-6

6.4.1 Incident Response Plans and Addendums

CSPs will provide, either as part of their *Incident Response Plan* or through an *Incident Response Plan Addendum,* their approach to fulfilling DoD Cyber Defense integration requirements. CSPs will make their plan or addendum available to DISA for review and approval as a condition of its PA and inclusion in the DoD Cloud Service Catalog. CSPs will update and deliver the *Incident*

[94] US-CERT: https://www.us-cert.gov/

Response Plan Addendum (if used) in conjunction with updates and deliveries of their *Incident Response Plan*, as required by the FedRAMP selected security control IR-1. A CSP must specifically address cyber incidents and data breaches, where a "breach" or cyber incident includes the loss of control, compromise, unauthorized acquisition, unauthorized access, or any similar term referring to situations where any unauthorized person has access or potential access to government data, whether in electronic or non-electronic form, for any unauthorized purpose. CSPs must ensure that the plan or addendum addresses all incidents regardless of the time, day, or location of the incident and must provide for notice to the Government of any breach of its data. The plan or addendum must incorporate any other policies or procedures that the Government may require to be followed in the event of an incident, including, but not limited to:

- To whom within the Government, the incident will be reported IAW the incident reporting process defined in Section 6.4.3, *Incident Reporting Mechanism*
- Specific steps to be taken in order to mitigate or remedy the incident, including time periods for taking such steps (e.g., reporting of Personally Identifiable Information (PII) data breaches within one hour, Negligent Disclosure of Classified Information (NDCIs) which are commonly referred to as spillages)
- How and under what circumstances any individuals or entities affected by an incident will be notified and by whom and
- Any other special instructions for handling computer security incidents affecting, or potentially affecting U.S. Government data; consistent with guidance and policy directives issued by DoD, NIST, US-CERT and CNSS for incident management, classification, and remediation; or other applicable law, regulation, order, or policy.

Corresponding Security Controls: IR-8

6.4.2 Information Requirements, Categories, Timelines, and Formats

Defending DoD missions and systems is a shared responsibility that requires all entities (CSPs; Cyber Defense entities (MCD, BCD); Mission Owners and Mission Administrators) to work collectively as a team. An event may be detected by any of following entities, depending upon the connection architecture (direct Internet or through a BCAP):

- CSP personnel through monitoring of their CSO (especially for PaaS/SaaS);
- Mission administrators or owners (includes the CSP for PaaS/SaaS);
- Supporting MCDs through their monitoring;
- Supporting BCDs via the CAP monitoring.

All entities must work together to quickly investigate and respond to events and incidents. In the course of a CSP performing Cyber Defense for its environments, CSPs will monitor their information systems and report relevant information to the MCD, focused on situations where any unauthorized person has access or potential access to government data.

CSP's reporting requirements to DoD will align with the reporting lexicon used by US-CERT for the broader Federal Government reporting requirements. Incident notifications should include a description of the incident and as much of the following information as possible:

- Contract information to include contract number, USG Contracting Officer(s) contact information, contract clearance level, etc.
- Contact information for the impacted and reporting organizations as well as the MCD.

- Details describing any vulnerabilities involved (i.e., Common Vulnerabilities and Exposures (CVE) identifiers)
- Date/Time of occurrence, including time zone
- Date/Time of detection and identification, including time zone
- Related indicators (e.g. hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures)
- Threat vectors, if known (see Threat Vector Taxonomy and Cause Analysis flowchart within the US-CERT Federal Incident Notification Guidelines)
- Prioritization factors (i.e. functional impact, information impact, and recoverability as defined flowchart within the US-CERT Federal Incident Notification Guidelines[95])
- Source and Destination Internet Protocol (IP) address, port, and protocol
- Operating System(s) affected
- Mitigating factors (e.g. full disk encryption or two-factor authentication)
- Mitigation actions taken, if applicable
- System Function(s) (e.g. web server, domain controller, or workstation)
- Physical system location(s) (e.g. Washington DC, Los Angeles, CA)
- Sources, methods, or tools used to identify the incident (e.g. Intrusion Detection System or audit log analysis)
- Any additional information relevant to the incident and not included above.

Initial incident reports should be submitted within one hour of discovery with follow-on information provided as available. Initial reports may be incomplete to facilitate communication and teamwork between the CSP and the supporting MCD/BCD entities. CSPs should balance the necessity of timely reporting (incomplete reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

NOTE: These requirements are applicable to all systems at all Information Impact Levels. The CSP must follow these requirements when integrating with the DoD Cyber Defense C2 and Network Operations (NetOps) structure. Mission Owners must include these requirements in the contract, even at Level 2.

Corresponding Security Controls: IR-5, IR-6, IR-8

6.4.3 Incident Reporting Mechanism

DoD CSP's (e.g., milCloud's) Cyber Defense providers will report all incidents using the Joint Incident Management System (JIMS) IAW normal DoD processes.

The following requirements are consistent with DFARS Clause 252.204-7012(d) as updated for Cloud Computing when finalized.

Level 2/4/5 Commercial CSPs will report all incidents via the on-line Defense Industrial Base (DIB) Cyber Incident Collection Format (ICF)[96]. Use of the on-line format is preferred. Access

[95] US-CERT Federal Incident Notification Guidelines: https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

to this format requires a DoD-approved medium assurance External Certificate Authority (ECA) certificate. If you are unable to access this format, please call (877) 838-2174 or email: DCISE@DC3.mil.

The CSP must include, for routing purposes, all MCD points of contact (POCs) for all DoD missions affected by the incident. This is in addition to any other POCs required by the tool for routing to contract managers, etc. The MCD, once the report is received, will initiate the DoD reporting process via JIMS.

When classified incident reporting is appropriate and directed, CSPs will use SIPRNet email or secure phone/fax to report and coordinate incidents as specified. Level 6 Commercial CSPs will report all incidents to the MCD using SIPRNet email or secure phone/fax to report and coordinate incidents as specified.

Existing notification mechanisms of a CSP that are already in place to communicate between the CSP and its customers for some or all classes of Cyber Defense information may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

Corresponding Security Controls: IR-6, IR-8

6.4.4 Digital Forensics in the Cloud and Support for Law Enforcement/Criminal Investigation

Incidents and compromises will happen. When they do, they must be reported and then forensically analyzed to gain detailed information regarding how it occurred how to prevent it or protect the system in the future, and potentially who is responsible. Incident information must be gathered and handled in a manner that will support legal prosecution if needed. As such it must be protected from alteration from the time it is captured until it is no longer needed. Support for forensics is shared between the Mission Owner and the CSP to various degrees depending on the service type.

Digital forensics in the cloud has many challenges as described by NIST in *Draft National Institute of Standards and Technology Interagency or Internal Report* (NISTIR) 8006, *Cloud Computing Forensic Science Challenges*.[97] This section of the CC SRG provides initial guidance regarding the DoD requirements for enabling and performing Cloud Forensics and supporting Law Enforcement and Criminal Investigation (LE/CE) activities.

The following requirements apply to all Information Impact Levels 2 through 6.

Corresponding Security Controls: IR-4, IR-5(1)

6.4.4.1 Malicious Software

CSPs or their subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall securely submit the malicious software to the MCD for analysis in addition to any other analysis organization employed by the CSP. The means of submission will be coordinated with the MCD. The DoD Cyber Defense community will use their analysis to

[96] DIBNet CS/IA Portal: http://dibnet.dod.mil/
[97] NISTIR 8006: http://csrc.nist.gov/publications/PubsDrafts.html

develop detection signatures and mitigation measures to be applied to DoD networks and Mission Owner's systems. Analysis results will be shared with the CSP if permissible and the appropriate communication channels exist.

Corresponding Security Controls: SI-3 (10)

6.4.4.2 Incident Information Collection, Preservation, and Protection

Under all service types including SaaS, when a CSP discovers a cyber-incident has occurred within infrastructure and/or CSO for which they are responsible, in conjunction with initial incident reporting, the CSP shall capture, preserve, and protect images and state of all known affected systems/servers/workstations supporting the CSO and the customer. This includes system logs, volatile memory captures, and hard drive (physical or virtual) images. The CSP shall also preserve and protect all relevant network logs, as well as all available network monitoring/packet capture data. This information must be collected as soon as possible after the discovery if not immediately.

The CSP will maintain captured incident information for at least 90 days from the submission of the required cyber incident report to allow DoD to request the information or decline interest. This requirement applies to the underlying infrastructure supporting IaaS, PaaS, and SaaS, the systems and applications managed by the CSP under PaaS, and all systems and applications under SaaS.

Under IaaS, when a Mission Owner discovers a cyber-incident has occurred within their systems/applications/virtual networks, they will work with their MCD and CSP to capture, preserve, and protect images and state of all known affected virtual machines which they manage as well as any network logs, and network monitoring/packet capture data generated by their virtual network(s). This includes system logs, volatile memory captures, and virtual hard drive images. While the virtual hard drive image of a compromised VM is typically easy to preserve as a new image is placed into service, tools run on the compromised VM before it is shut down are typically used to capture and package the system logs and/or volatile memory and detailed procedures are followed. An example of this is the DISA Incident Response and Recovery Team's (IRRT) First Responder's Guide and web page[98] which makes software tools available for Windows and UNIX/Linux based systems to collect the necessary supporting information. These tools work within the VM and the volatile memory allocated to it. They will not compromise other customers' information or VMs running on the same physical hardware which may be a concern for other tools. Each MCD is required to have and use similar procedures and tools. The Mission Owner and/or MCD must subsequently coordinate with the CSP to collect relevant infrastructure logs in support of investigating the incident. Alternately, the CSP may/should also provide similar tools/capabilities that will work in their environment.

Under PaaS and SaaS, a Mission Owner, their MCD, or the CSP may detect an incident. Each party must work with the others to collect the necessary forensic information from the areas of the service each manages. It may be unlikely that the Mission Owner will be able to run the tools discussed under IaaS above, however, the CSP must provide similar tools/capabilities that will work in their environment.

[98] DISA IRRT Web site: https://blogs.intelink.gov/blogs/_disairrt (CAC/PIV PKI required)

Under PaaS, if the Mission Owner manages their contracted servers (VMs or otherwise) OS and platform applications, it is their responsibility to perform the capture, preserve, and protect functions in coordination with their MCD as described under IaaS on their own or using tools provided by the CSP. If, on the other hand, the CSP manages the CSO servers OS and/or platform applications, then the CSP must perform the capture, preserve, and protect functions in conjunction with their CDSP. The CSP will then share their results with the Mission Owners MCD.

Under SaaS, the CSP must perform the capture, preserve, and protect functions in conjunction with their CDSP. The CSP will then share their results with the Mission Owner's MCD.

All captured incident information is digital evidence. All digital evidence, when copied / captured from the system, the original and copied information must be hashed to validate the integrity of the copy initially and in the future.

To be effective all incident capture should be performed using automation IAW IR-5(1). The CSP must provide an automated capability that supports incident capture and protection, which must support the CSP's investigation of incidents within their own infrastructure and in customer's CSO environments. An interface to the capability must be made available to the customer in support of the customer's incident response activities as needed in their environments within the CSO. All such automation must capture the information in a manner that segregates captured information by customer such that non-DoD or non-Federal information is not revealed to the incident response team or forensic / LE investigators. Likewise the information relating to the government environment must be segregated from the information captured from the CSP's underlying infrastructure. Once the information is captured, the automation must create one or more hashes of the data such that changes to it can be detected. The automation must then encrypt the data to preserve its confidentiality and integrity. Captured Information captured from the CSP's underlying infrastructure will be encrypted separately from the information captured from the Government's environment. Encryption keys will be provided to the forensics analysists and stored in such a manner that only the Government has access to the keys for the information captured from the Government's environment and the CSP has access to captured data from the CSP's underlying infrastructure.

NOTE: At this time some of the tools provided on the DISA IRRT website (more specifically Oscar) incorporate licensed software and may not be used by other organizations other than as directed by the DISA IRRT.

Mission Owners must reflect these requirements in their contract /SLA with the CSP delineating specific responsibilities between the CSP and Mission Owner/MCD.

Corresponding Security Controls: IR-4, IR-5(1), IR-8, SI-12

6.4.4.3 Forensics/Incident Information Chain-of-Custody for LE/CI

According to NISTIR 8006, Chain-of-custody is defined in legal contexts as the chronological documentation of evidence handling, which is required to avoid allegations of evidence tampering or misconduct. In the event the incident discovered by the CSP or Mission Owner was maliciously caused by an individual, maintaining the chain of custody over the information is critical to being able to legally reprimand or prosecute the responsible individual or organization.

To support LE/CI investigations, the chain-of-custody of the captured data should be documented from end-to-end, person-to-person starting when the incident investigation begins. The individual that captures each piece or portion of the information initiates this documentation and each individual that subsequently handles the information or media containing it must continue the documentation. Chain-of custody-forms are available on the DISA IRRT web site noted above or from law enforcement. While chain-of-custody documentation is important and recommended; initiating the chain-of-custody forms and procedures may only be required if the incident warrants the notification of law enforcement. In that case, the chain-of-custody forms will be initiated by law enforcement officers. If requested or subpoenaed, the CSP will make their employees available to provide attestation either via affidavits or expert testimony on the CSP's chain-of-custody and forensic data capture/collection methods.

Corresponding Security Controls: SI-12

6.4.4.4 Digital Forensics Support by CSP toward PA Award

CSPs will be evaluated for their ability to support the requirements above that are incumbent upon the CSP and for their ability to support requirements that are incumbent upon the Mission Owner particularly in the area of system image and state preservation. This includes capabilities and tools to support the capture and preservation of system logs, volatile memory captures, and hard drive (physical or virtual) images by the Mission Owner or CSP. The CSP must document their capability to support digital forensics in their Security Plan. CSP Forensics Support capabilities and their acceptability will be documented in the information supporting the PA.

6.5 Warning, Tactical Directives, and Orders

The DoD Cyber Defense C2 structure, in order to effectively defend DoD information systems that are networked globally across a diverse set of environments. Each of these environments must defend the network and ensure the security of computing and communication systems. It is critical that certain information be disseminated and that actions and supporting countermeasures can be directed from higher levels of command to network defenders (which include CSPs supporting defense of their CSOs).

The DoD cyber chain of command for CSPs is represented in Figure 10. USCYBERCOM, at Tier 1, disseminates Warnings, Tactical Directives, and Orders to both the BCD and MCDs (all Tier 2). The BCD entities will analyze them for their applicability to individual CSPs, and then communicate with USCYBERCOM and the CSPs as appropriate. CSPs will coordinate with the BCD, MCD, and Mission Owners as contracted to implement the provided guidance and countermeasures.

CSPs must be able to receive, act upon, and report compliance with directives and notifications sent by Cyber Defense Tier 2 (MCD or BCD), as required by FedRAMP selected security control SI-5.

6.6 Continuous Monitoring / Plans of Action and Milestones (POA&Ms)

Understanding existing vulnerabilities and risks within the enterprise is a key component in performing effective Cyber Defense analysis. The vulnerability reports and POA&Ms developed by the CSPs as part of continuous monitoring requirements supporting both FedRAMP and FedRAMP+ requirements will be made available to DISA's cloud services support team and

subsequently to the MCD and BCD providers for their collective use in providing Cyber Defense.

For both FedRAMP and FedRAMP+ requirements, high and critical risk findings must be mitigated within 30 days. Moderate findings must be mitigated within 90 days.

Corresponding Security Controls: CA-5, CA-7

6.7 Notice of Scheduled Outages

Planned outages affecting mission systems are to be coordinated through the Mission Owner; with the goal of minimizing impacts to the operational community. An approved outage is referred to as an Authorized Services Interruption (ASI). CSPs must notify all affected MCD providers of ASIs under their control when an outage starts and upon return to service. Outages or changes that affect more than one mission environment must be reported by the MCD to the BCD to enable broader situational awareness across all MCD providers. Mission owners and administrators are responsible for the same notifications to the MCD when the ASI is under their control.

6.8 PKI for Cyber Defense Purposes

The DoD PKI program provides assurances of an individual's identity, which is important in sharing information regarding C2 and Cyber Defense functions. This section outlines requirements for establishing trusted identities for CSP personnel communicating securely with DoD Cyber Defense personnel. Once an incident is reported through the process identified in Section 6.4.3, *Incident Reporting Mechanism*, and in the event signed or encrypted email is to be used as the subsequent communications method, DoD PKI certificates will be required as follows:

Impact Level 2 through 5: CSPs must preferably have either a DoD PKI certificate or a DoD-approved PKI credential for each person that needs to communicate with DoD via encrypted email. For more information on DoD-approved credentials, please see the IASE PKI/ECA web page[99] and PKI/PK Enabling (PKE) web page[100]. Equivalent alternative measures will be assessed on a case by case basis.

Impact Level 6: CSPs serving Level 6 systems will already have SIPRNet tokens / NSS PKI certificates for their system administrators by virtue of the connection to SIPRNet. Incident response and Cyber Defense personnel will use SIPRNet tokens/certificates to communicate with DoD via encrypted email.

6.9 Vulnerability and Threat Information Sharing

Vulnerability and threat information sharing is a highly effective way for DoD to help CSPs protect and defend DoD information housed or processed in their service offerings. Government sources such as US-CERT and USCYBERCOM provide detailed vulnerability information. Several commercial sources also provide supplemental information that can be used by CSPs in further defending their infrastructure. CSPs are encouraged to leverage such knowledge sources.

[99] IASE PKI/ECA page: http://iase.disa.mil/pki/eca/Pages/index.aspx
[100] IASE PKI/PKE Page: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx

However, much of the information that the DoD can provide to CSPs is classified. An avenue to obtain such information follows:

The Defense Industrial Base Cyber Security / Information Assurance Program[101] (DIB CS/IA) is a program to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. Under this voluntary public-private cybersecurity partnership, DoD and participating DIB companies share unclassified and classified cyber threat information, best practices and mitigation strategies. While cyber incident reporting is an important component to the success of this partnership, the real value of the program is collaboration that is key to making DoD information more secure. Membership in DIB CS/IA enables DIB participants to acquire access to DIBNet-U and DIBNet-S, the unclassified and classified networks used for data sharing and collaboration. Access to DIBNet provides CSPs with access to CYBERCOM notifications, classified email, and the DIB web portals.

Access to DIBNet provides CSPs with access to both classified and unclassified cyber threat information, including mitigation strategies. DIB CS/IA program membership is voluntary, although cyber incident reporting as described in Section 6.4.3, *Incident Reporting Mechanism* is mandatory. Eligible CSPs are encouraged to join the voluntary DIB CS/IA program to facilitate their protection of infrastructure that hosts higher-value DoD data and systems.

NOTE: DoD CSPs are already integrated into the Cyber Defense communications architecture and receive unclassified CYBERCOM notifications via established channels.

[101] DIBNet CS/IA Portal: http://dibnet.dod.mil/staticweb/index.html

Appendix A References

1. Public Law 93-579, as codified at 5 U.S.C. 552a, Privacy Act of 1974
http://www.archives.gov/about/laws/privacy-act-1974.html
2. Public Law 104-191, Health Insurance Portability and Accountability (HIPAA) Act of 1996
http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html
3. Public Law 83-703, Atomic Energy Act of 1954, as amended,
http://pbadupws.nrc.gov/docs/ML1327/ML13274A489.pdf#page=23
4. 22 Code of Federal Regulations (CFR), 22 CFR 120.15 – US Persons, 120-16 – Foreign persons,
https://www.gpo.gov/fdsys/pkg/CFR-2011-title22-vol1/pdf/CFR-2011-title22-vol1-sec120-15.pdf
5. 8 U.S. Code § 1408 - Nationals but not citizens of the United States at birth,
https://www.gpo.gov/fdsys/pkg/USCODE-2010-title8/pdf/USCODE-2010-title8-chap12-subchapIII-partI-sec1408.pdf
6. Executive Order 13526: Classified National Security Information, dated 29 December 2009.
http://www.archives.gov/isoo/policy-documents/cnsi-eo.html
7. Executive Order 12829 – National Industrial Security Program, January 1993.
http://www.archives.gov/isoo/policy-documents/eo-12829.html
8. Executive Order 13556 - Controlled Unclassified Information.
https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
9. EO 12958, Classified National Security Information (April 17, 1995) as amended by EO 13292.
http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html
10. 48 Code of Federal Regulations (CFR) Subpart 4.4 - Safeguarding Classified Information within Industry.
https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4-subpart4-4
11. Federal Acquisition Regulations (FAR) section 52.204-2 - Security Requirements.
https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf
12. NIST FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
13. NIST SP 500-292: NIST Cloud Computing Reference Architecture, dated September 2011.
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
14. NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, Revision 4, dated April 2013.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Note: http://csrc.nist.gov/publications/PubsSPs.html contains additional documents relating to SP 800-53.

15. NIST SP 800-59: Guideline for Identifying an Information System as a National Security System, dated August 2003.
http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf
16. NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, dated October 2008.
http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
17. NIST SP 800-88, Revision 1: Guidelines for Media Sanitization, dated September 2012.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
18. NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), dated April 2010.
http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
19. NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, dated December 2011.
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
20. NIST SP 800-145: The NIST Definition of Cloud Computing, dated September 2011.
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
21. NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems, dated February 2010.
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
22. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, dated June 2015.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
23. CNSS Instruction 4009: National Information Assurance (IA) Glossary, dated 30 April 2010.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm
24. CNSS Instruction 1253: Security Categorization and Control Selection for National Security Systems, dated 27 March 2014.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm
25. CNSS Instruction No.1253F, Attachment 5: Classified Information Overlay dated 09 May 2014.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm
26. CNSS Instruction No.1253F, Attachment 6: Privacy Overlay dated 20 April 2015.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm
27. DoD Chief Information Officer, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014.
http://iase.disa.mil/Documents/commercial_cloud_computing_services.pdf
28. DoD Instruction 8500.01: Cybersecurity, dated 14 March 2014.
http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

29. DoD Instruction 8510.01: Risk Management Framework (RMF) For DoD Information Technology (IT), dated 12 March 2014.
http://dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

30. DoD Instruction 8520.03: Identity Authentication for Information Systems, dated 13 May, 2011.
http://dtic.mil/whs/directives/corres/pdf/852003p.pdf

31. DoD Instruction 8551.01: Ports, Protocols, and Services Management (PPSM), May 28, 2014.
http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf

32. DoD Instruction 8410.01, Internet Domain Name Use and Approval, dated April 14, 2008.
http://www.dtic.mil/whs/directives/corres/pdf/841001p.pdf

33. DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)", March 9, 2001.
https://whsddpubs.dtic.mil/corres/pdf/O85302p.pdf (PKI required)

NOTE: DoD Instruction O-8530.2 has been updated and is soon to be replaced with the following:

34. DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations"
http://www.dtic.mil/whs/directives/corres/pdf/853001p.pdf

35. DoD Joint Publication 3-12 (R), "Cyberspace Operations"
http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

36. DoD Instruction 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems, June 6, 2012.
http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf

37. DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense
http://www.dtic.mil/whs/directives/corres/pdf/832007p.pdf

38. DoD 5220.22-R: Industrial Security Regulation (ISR), dated December 1985.
http://www.dtic.mil/whs/directives/corres/pdf/522022r.pdf

39. DoD Instruction 5220.22: National Industrial Security Program, dated March 2011.
http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf

40. DoD Manual 5220.22 Manual: National Industrial Security Program: Operating Manual (NISPOM), dated march 2013.
http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf

41. DoD Instruction 5200.01: DoD Information Security Program and Protection of SCI, dated June 2011.
http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

42. DoD Manual 5200.01 Vol 1: DoD Information Security Program: Overview, Classification and Declassification, dated February 2012.
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf

43. DoD Manual 5200.01 Vol 2: DoD Information Security Program: Marking of Classified Information, dated March 2013.
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf

44. DoD Manual 5200.01 Vol 3: DoD Information Security Program: Protection of Classified Information, dated March 2013.
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

45. DoD Instruction 5200.02: DoD Personnel Security Program (PSP), Change 1 dated September 2014.
http://www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf

46. DoD Manual 5200.2-R: Personnel Security Program, dated February 1996.
http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

47. CJCSM 6510.01B: Chairman of the Joint Chiefs of Staff Manual: Cyber Incident Handling Program, dated 10 July 2012. (Current as of 18 December 2014).
http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

48. DSS Facility Clearance Branch.
http://www.dss.mil/isp/fac_clear/fac_clear.html

49. DoD ECA PKI Certificate.
http://iase.disa.mil/pki/eca/Pages/index.aspx

50. OPM Position Designation System 2010.
http://www.opm.gov/investigations/background-investigations/position-designation-tool/oct2010.pdf

51. Federal Risk and Authorization Management Program (FedRAMP) Home Page.
https://www.fedramp.gov/

52. FedRAMP Control Specific Contract Clauses v2, June 6, 2014.
http://www.fedramp.gov/resources/documents

53. Defense Information Systems Agency, the Security Technical Implementation Guide (STIG) Home Page.
http://iase.disa.mil/stigs/Pages/index.aspx

54. Defense Information Systems Agency, DoD Cloud Services Support website.
http://disa.mil/Services/DoD-Cloud-Broker

55. Guide to Understanding FedRAMP.
https://www.fedramp.gov/resources/documents/

56. FedRAMP Continuous Monitoring Strategy Guide.
https://www.fedramp.gov/resources/documents/

57. FedRAMP Control Specific Contract Clauses v2, June 6, 2014.
https://www.fedramp.gov/resources/documents/

58. OPM Position Designation System document, Oct 2010.
http://www.opm.gov/investigations/background-investigations/position-designation-tool/oct2010.pdf

59. OPM Position Designation Tool.
http://www.opm.gov/investigations/background-investigations/position-designation-tool/

This page is intentionally blank.

Appendix B Glossary

Authenticity: As defined in CNSSI-4009, *"The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator."*

Availability: As defined in CNSSI-4009, *"The property of being accessible and useable upon demand by an authorized entity."*

Classified Information: As defined in CNSSI-4009, *"Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."*

CDSP: Computer Network Defense Service Provider

CSM: Cloud Security Model. The CSM is the document that preceded the CC SRG and has since been deprecated.

Dedicated infrastructure: Refers to the cloud service infrastructure being dedicated to serving a single customer organization or a specific group of customer organizations.

Community Cloud: A multi-tenant cloud in which services are provided for the exclusive use of the DoD and Federal Government organizations. Resources providing the cloud services must be dedicated to Federal Government use and require physical separation from non-DoD/non-Federal customers.

Confidentiality: As defined in CNSSI-4009, *"The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information."*

Cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident.

Incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Infrastructure as a Service (IaaS): As defined in NIST SP 800-145, *"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."*

Integrity: As defined in CNSSI-4009, *"The property whereby an entity has not been modified in an unauthorized manner."*

JAB: Joint Authorization Board. The primary governance and decision-making body for the FedRAMP program.

Mission Owner: A DoD Cloud Consumer. As defined in NIST SP 500-292, "A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider."

Non-Repudiation: As defined in CNSSI-4009, *"Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information."*

Platform as a Service (PaaS): As defined in NIST SP 800-145, *"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment."*

Private Cloud: Cloud in which services are provided for the exclusive use of the DoD; supporting multiple DoD tenants or DoD sponsored tenants in the same cloud. The DoD maintains ultimate authority over the usage of the cloud services, and any non-DoD use of services must be authorized and sponsored through the DoD. Resources providing the cloud services must be dedicated to DoD use and have physical separation from resources not dedicated to DoD use.

Restoration: The return of something to a former, original, normal, or unimpaired condition.

SCA: Security Control Assessor. As defined in NIST SP 800-37, *"The individual, group, or organization responsible for conducting a security control assessment."*

Software as a Service (SaaS): As defined in NIST SP 800-145, *"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."*

Spillage or Data Spill: an unauthorized transfer of classified information or Controlled Unclassified Information to an information system that is not accredited for the applicable security level of the data or information.

Appendix C Roles and Responsibilities

Table 7 provides a summary of the major roles and responsibilities in implementation of the CC SRG.

Table 7 - Roles and Responsibilities

Role	Responsibility
DISA	• Provide security requirements guidelines (SRGs) and Security Technical Implementation Guidance (STIGs) for DoD cloud computing • Assess CSP's Service Offerings and 3PAO results for consideration in awarding a DoD Provisional Authorization • Issue DoD Provisional Authorizations • Develop and maintain a DoD Cloud Access Point (CAP). • Provide DoDIN Cyber Defense capabilities and maintain a Cyber Defense concept of operations (CONOPS). • Provide technical support for the DoD CIO's role on the FedRAMP Joint Authorization Board • Provide a catalog of DoD cloud services • Maintain a registry of DoD Components using commercial cloud services. • Support the DoDIN Waiver Process • Receives CSP's continuous monitoring products and passes them to the appropriate entities within DoD • Serve as the DoD CDSP certifier
Cloud Service Provider (CSP)	• Commercial vendor or Federal organization offering or providing cloud services (Includes DoD CSPs) • Provides Cloud Service Offerings for mission use • Provides CDSP services (all tiers) for their infrastructure and service offerings
Cloud Access Point (CAP)	• Provided by DISA or other DoD Component • Protect DoD missions from vulnerabilities or risk that may affect operations in a CSP environment • Provide perimeter defenses and sensing for applications hosted in the commercial cloud service
DoD Chief Information Officer (DoD CIO)	• Official approving authority for all CAPs
FedRAMP Joint Authorization Board (JAB)	• Reviews CSP security assessment packages under the FedRAMP program • Grants FedRAMP Provisional Authorizations • Ensures that FedRAMP Provisional Authorizations are reviewed and updated regularly • Approves accreditation criteria for third party assessment organizations (3PAOs)
Third Party Assessment Organizations (3PAO)	• Accredited by American Association for Laboratory Accreditation (A2LA) and with final approval by FedRAMP PMO • Contracted by CSP • Independently performs security assessments of a CSP cloud offering and creates security assessment package artifacts in accordance with FedRAMP requirements • May perform continuous monitoring of CSP systems • May independently assess a CSP's compliance to DoD FedRAMP+ security controls and other requirements

Role	Responsibility
DISA Cloud SCA	• May independently assess a CSP's compliance to DoD FedRAMP+ security controls and other requirements if not performed by a 3PAO • May assess a CSP's compliance to FedRAMP security controls for DoD CSPs if not done by another DoD SCA • May assess a CSP's compliance to FedRAMP security controls for Commercial CSPs undergoing a DoD assessment outside of FedRAMP if not done by another DoD SCA • Advises the DISA AO regarding PA award through the assessment of CSP SARs and the development of a Certification Recommendation • Serves as FedRAMP Technical Advisor to the DoD CIO in his/her role as JAB tri-chair
DoD Cloud SCA (Other than DISA)	• May assess a CSP's compliance to FedRAMP and FedRAMP+ security controls for DoD or non-DoD CSPs undergoing a DoD assessment outside of FedRAMP (if not done by DISA) toward awarding an DoD PA and component Agency ATO.
DISA Authorizing Official (AO)	• Official approving PA for a CSP's Service Offerings for DoD use
DISA Cyber Defense Functions	• Perform cross-CAP correlation and analysis of event/data. • Direct C2 actions regarding DoDIN-wide incident and system health reporting involving a CAP or CSP. • For DoDIN-wide incidents, establish and maintain external communications with the CSP and ensure internal DoD communications are established between all entities which include the MCD and BCD. • Interface with US-CERT to obtain relevant CSP information; ensures cross-sharing of information across all BCD/MCD entities.
DoD Component Authorizing Official (AO)	• Official approving ATOs for Mission Owner's systems/applications • Reviews PA documentation to understand residual risk
Mission Owner (CSP's DoD Cloud Customer DoD Cloud Consumer)	• DoD entity that acquires cloud services in support of its mission • Reviews DoD PA documentation to understand residual risk • Performs assessment to issue ATO for their mission systems/applications • Ensures Tier 2 Mission Computer Network Defense (MCD) Service Provider is identified and funded • Serves as Cyber Defense Tier 3 for their mission systems/applications • Ensures CSP requirements for Cyber Defense and other SRG requirements are included in any cloud contracts • Registers ports and protocols with the PPSM Office
Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT)	• Receives incident reports from CSP as mandated by FedRAMP. • Responsible for coordination across non-DoD agencies
Computer Network Defense Service Provider (CDSP)	• Provides Cyber Defense services and Command and Control (C2) direction addressing the protection of the network, detection of threats, and response to incidents.
United States Cyber Command (USCYBERCOM) / JFHQ-DoDIN • DoD Tier 1 CDSP	• Notify and Coordinate as appropriate with US-CERT, Intelligence Community, Law Enforcement, and other Federal Agencies • Provides Cyber Defense services and Command and Control (C2) direction for the entire DoDIN and all DoD information systems

Role	Responsibility
Boundary Cyber Defense (BCD) • DoD Tier 2 CDSP	• Monitors and defends the connections to/from off-premises CSPs at the Cloud Access Point (CAP) • Provides cross-CSP analysis capabilities or entities • Communicates with Cyber Defense Tier 1 and Tier 2 entities • Provides MCDs timely access to BCD-collected indications and warnings relevant to MCD subscribers.
Mission Cyber Defense (MCD) • DoD Tier 2 CDSP	• Provides Cyber Defense / C2 services to specific Mission Owner's systems/applications and virtual networks • Serves as the DoD Cyber Defense / C2 point of contact for the CSP • Communicates with Cyber Defense Tier 2 and Tier 3 entities

This page is intentionally blank.

Appendix D CSP Assessment Parameter Values for PA

Table 8 provides a listing of only the FedRAMP and FedRAMP+ C/CEs that require parameter values. These C/CEs and associated parameter values are published here as a benchmark for CSPs and will be used for CSP assessment toward receiving a PA. It is not a complete list of all FedRAMP moderate and FedRAMP+ C/CEs that a CSP must meet. The full C/CEs text is included to provide full context for the selection or value being addressed.

Many parameter values are not defined by DoD or FedRAMP since they may change depending on the CSP organization and/or CSO. This makes it impossible to define all parameter values for all cases in this SRG. For parameter values not defined in Table 8 as indicated by the lack of a reference in the right hand column to the parameter in the left hand column, the CSP must define the parameter values in the Security Plan along with the details on how the C/CE is met for the DoD to assess and the DISA AO to accept/approve for the DoD PA.

NOTE: For some C/CEs none of the required parameter selections/values were defined by DoD or FedRAMP. As such the right column cell in the table is blank. The associated parameter values are treated as noted above with the CSP defining the value for assessment.

In many cases, DoD and FedRAMP defined different values for control parameters. In such cases, and as displayed, the more stringent parameter values will be required for a DoD PA at Impact Levels 4-6. Impact Level 2 CSOs will be assessed using the FedRAMP values. Controls with different parameter values for Impact Level 2 as compared to Impact Levels 4-6 are noted in the table. The CSP may offer alternate values or methods of meeting a control for consideration.

Mission Owners must use, define, and/or tailor the parameter values for the applications they instantiate in IaaS/PaaS cloud services in accordance with the values defined by the DoD RMF TAG. DoD/FedRAMP predefined and CSP defined parameter values assessed for DoD PA award are inherited by the Mission Owners' systems/applications. If the Mission Owner needs alternate values for these inherited values, they must be negotiated with the CSP and reflect the change in their SLA/contract.

NOTE: DoD Components / Mission Owners may tailor this set of values by altering existing or defining additional selections/values when publishing RFPs and executing contracts. Mission owners must either accept the values documented in the CSP's Security Plan and accepted by the DISA AO as reflected in the PA or negotiate for alrernate values and include them in their contract/SLA.

Table 9 provides a listing of only the C/CEs listed in Table 3 - Security Controls/Enhancements to be addressed in the Contract/SLA that require parameter values. These are provided to inform Mission Owners and CSPs of the DoD values associated with the parameters. For parameter values not defined in Table 9 as indicated by the lack of a reference in the right hand column to the parameter in the left hand column, the Mission Owner must assign the value in their contract/SLA when selecting the C/CE, accept a CSP assigned value, or negotiate the value with the CSP.

Table 8 – FedRAMP M / FedRMP+ Control / Enhancement Parameter Values for PA Assessment

Control/Enhancement text	Value
AC-1; ACCESS CONTROL; Access Control Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy **[Assignment: organization-defined frequency]**; and 2. Access control procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-100.	AC-1 **Impact Levels 4-6:** a. all personnel Source: DoD RMF TAG ---------- **Impact Level 2:** b.1 at least every 3 years **All Impact Levels:** b.2 at least annually Source: FedRAMP v2 ----------
AC-2; ACCESS CONTROL; Account Management: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: **[Assignment: organization-defined information system account types]**; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by **[Assignment: organization-defined personnel or roles]** for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with **[Assignment: organization-defined procedures or conditions]**; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements **[Assignment: organization-defined frequency]**; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. References: None.	AC-2 **Impact Levels 4-6:** e. ISSM or ISSO Source: DoD RMF TAG ---------- **All Impact Levels:** j at least annually Source: FedRAMP v2 ----------

AC-2 (2); ACCESS CONTROL; Account Management - Enhancement: Removal Of Temporary Emergency Accounts The information system automatically **[Selection:** **- removes;** **- disables** **]** temporary and emergency accounts after **[Assignment: organization-defined time period for each type of account]**. References: None.	AC-2 (2) **Impact Levels 4-6:** For temporary user accounts: 72 hours For emergency admin accounts: never (see supplemental recommendation) Source: DoD RMF TAG --- **Impact Level 2:** [No more than 30 days for temporary and emergency account types] Source: FedRAMP v2 ---
AC-2 (3); ACCESS CONTROL; Account Management - Enhancement: Disable Inactive Accounts The information system automatically disables inactive accounts after **[Assignment: organization-defined time period]**. References: None.	AC-2 (3) **Impact Levels 4-6:** 35 days Source: DoD RMF TAG --- **Impact Level 2:** 90 days for user accounts Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Authorizing Official.
AC-2 (4); ACCESS CONTROL; Account Management - Enhancement: Automated Audit Actions The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies **[Assignment: organization-defined personnel or roles]**. References: None.	AC-2 (4) **Impact Levels 4-6:** System administrator and ISSO Source: DoD RMF TAG ---
AC-2 (5); ACCESS CONTROL; Account Management - Enhancement: Inactivity Logout The organization requires that users log out when **[Assignment: organization-defined time-period of expected inactivity or description of when to log out].** References: None.	AC-2 (5) **Impact Levels 4-6:** At the end of the users standard work period unless otherwise defined in formal organizational policy. Source: DoD RMF TAG ---
AC-2 (7); ACCESS CONTROL; Account Management - Enhancement: Role-Based Schemes The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes **[Assignment: organization-defined actions]** when privileged role assignments are no longer appropriate. References: None.	AC-2 (7) **Impact Levels 4-6:** c. Disables (or revokes) privileged user account Source: DoD RMF TAG ---

AC-2 (9); ACCESS CONTROL; Account Management - Enhancement: Restrictions On Use Of Shared Groups / Accounts The organization only permits the use of shared/group accounts that meet **[Assignment: organization-defined conditions for establishing shared/group accounts].** References: None.	AC-2 (9) **All Impact Levels:** In support of auditing and accountability, shared/group accounts are not permitted unless the requirement to uniquely attribute user activity to the account is implemented; exceptions may be approved on a case-by-case basis. Personal accounts will not be shared. Source: DoD best practice, SRGs and STIGs, CNSSI 1253 Privacy Overlay. --- **FedRAMP Additional Requirements and Guidance:** Required if shared/group accounts are deployed
AC-2 (12); ACCESS CONTROL; Account Management - Enhancement: Account Monitoring /Atypical Usage The organization: (a) Monitors information system accounts for **[Assignment: organization-defined atypical use]**; and (b) Reports atypical usage of information system accounts to **[Assignment: organization-defined personnel or roles]**. References: None.	AC-2 (12) **Impact Levels 4-6:** b. at a minimum, the ISSO Source: DoD RMF TAG --- **All Impact Levels:** **FedRAMP Additional Requirements and Guidance:** AC-2 (12)(a) and AC-2 (12)(b) Additional FedRAMP Requirements and Guidance: Required for privileged accounts.
AC-4; ACCESS CONTROL; Information Flow Enforcement: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on **[Assignment: organization-defined information flow control policies]**. References: Web: ucdmo.gov	
AC-4 (21); ACCESS CONTROL; Information Flow Enforcement - Enhancement: Physical / Logical Separation Of Information Flows The information system separates information flows logically or physically using **[Assignment: organization-defined mechanisms and/or techniques]** to accomplish **[Assignment: organization-defined required separations by types of information]**. References: None.	
AC-5; ACCESS CONTROL; Separation Of Duties: The organization: a. Separates **[Assignment: organization-defined duties of individuals]**; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. References: None.	

AC-6 (1); ACCESS CONTROL; Least Privilege - Enhancement: Authorize Access To Security Functions The organization explicitly authorizes access to **[Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]**. References: None.	AC-6 (1) **Impact Levels 4-6:** all functions not publicly accessible and all security-relevant information not publicly available Source: DoD RMF TAG ----------
AC-6 (2); ACCESS CONTROL; Least Privilege - Enhancement: Non-Privileged Access For Non-security Functions The organization requires that users of information system accounts, or roles, with access to **[Assignment: organization-defined security functions or security-relevant information]**, use non-privileged accounts, or roles, when accessing non-security functions. References: None.	AC-6 (2) **All Impact Levels:** all security functions Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** AC-6 (2). Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.
AC-6 (5); ACCESS CONTROL; Least Privilege - Enhancement: Privileged Accounts The organization restricts privileged accounts on the information system to **[Assignment: organization-defined personnel or roles]**. References: None.	
AC-6 (7); ACCESS CONTROL; Least Privilege - Enhancement: Review Of User Privileges The organization: (a) Reviews **[Assignment: organization-defined frequency]** the privileges assigned to **[Assignment: organization-defined roles or classes of users]** to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs. References: None.	AC-6 (7) **Impact Levels 4-6:** a. at a minimum, annually a. all users Source: DoD RMF TAG ----------
AC-6 (8); ACCESS CONTROL; Least Privilege - Enhancement: Privilege Levels For Code Execution The information system prevents **[Assignment: organization-defined software]** from executing at higher privilege levels than users executing the software. References: None.	AC-6 (8) **Impact Levels 4-6:** any software except software explicitly documented Source: DoD RMF TAG ----------

AC-7; ACCESS CONTROL; Unsuccessful Login Attempts: The information system: a. Enforces a limit of **[Assignment: organization-defined number]** consecutive invalid login attempts by a user during a **[Assignment: organization-defined time period]**; and b. Automatically **[Selection:** **- locks the account/node for an** **[Assignment: organization-defined time period];** **- locks the account/node until released by an administrator;** **- delays next login prompt according to** **[Assignment: organization-defined delay algorithm]** **]** when the maximum number of unsuccessful attempts is exceeded. References: None.	AC-7 **Impact Level 2:** AC-7a [not more than three] [fifteen minutes] AC-7b [locks the account/node for thirty minutes] Source: FedRAMP v2 --- **Impact Levels 4-6:** a1. Three a2. 15 minutes b1. locks the account/node b2. Until released by an administrator b3. Minimum of 5 seconds Source: DoD RMF TAG ---
AC-8; ACCESS CONTROL; System Use Notification: The information system: a. Displays to users **[Assignment: organization-defined system use notification message or banner]** before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information **[Assignment: organization-defined conditions]**, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. References: None.	AC-8 **Impact Levels 4-6:** a. The CSO must have a capability to support the DoD banner as defined in DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 c. The CSO must have a capability to support the DoD banner under conditions as defined in DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 Source: DoD RMF TAG --- **Impact Level 2:** See Additional Requirements and Guidance. Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Authorizing Official (AO). Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the AO. Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided. Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the AO.

AC-10; ACCESS CONTROL; Concurrent Session Control: The information system limits the number of concurrent sessions for each **[Assignment: organization-defined account and/or account type]** to **[Assignment: organization-defined number]**. References: None.	AC-10 **Impact Levels 4-6:** all account types and/or accounts Source: DoD RMF TAG ---------- **Impact Level 2:** three (3) sessions for privileged access and two (2) sessions for non-privileged access Source: FedRAMP v2 ----------
AC-11; ACCESS CONTROL; Session Lock: The information system: a. Prevents further access to the system by initiating a session lock after **[Assignment: organization-defined time period]** of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. References: OMB Memorandum 06-16.	AC-11 **All Impact Levels:** a. 15 minutes Source: DoD RMF TAG and FedRAMP v2 ----------
AC-12; ACCESS CONTROL; Session Termination: The information system automatically terminates a user session after **[Assignment: organization-defined conditions or trigger events requiring session disconnect]**. References: None.	
AC-14; ACCESS CONTROL; Permitted Actions Without Identification Or Authentication: The organization: a. Identifies **[Assignment: organization-defined user actions]** that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication. References: None.	
AC-17 (3); ACCESS CONTROL; Remote Access - Enhancement: Managed Access Control Points The information system routes all remote accesses through Identifies **[Assignment: organization-defined number]** managed network access control points. References: None.	AC-17 (3) **Impact Levels 4-6:** Level 4/5: Off-Premises CSP infrastructure must connect to DoD customers via one or more external DoDIN Cloud Access Points (CAPs). Level 4/5: On-Premises Commercial CSP infrastructure must connect to DoD customers via one or more Internal DoDIN Cloud Access Points (CAPs).Not appropriate for DoD to define for all CSP's infrastructure or service offerings. The CSP defines the value and the DISA AO approves and/or accepts Source: DoD RMF TAG ----------

AC-17 (4); ACCESS CONTROL; Remote Access - Enhancement: Privileged Commands / Access The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for **[Assignment: organization-defined needs];** and (b) Documents the rationale for such access in the security plan for the information system. References: None.	
AC-17 (9); ACCESS CONTROL; Remote Access - Enhancement: Disconnect / Disable Access The organization provides the capability to expeditiously disconnect or disable remote access to the information system within **[Assignment: organization-defined time period]**. References: None.	AC-17 (9) **Impact Levels 4-6:** immediately Source: DoD RMF TAG --- **Impact Level 2:** no greater than 15 minutes Source: FedRAMP v2 ---
AC-19 (5); ACCESS CONTROL; Access Control For Mobile Devices - Enhancement: Full Device / Container- Based Encryption The organization employs **[Selection:** **- full-device encryption;** **- container encryption** **]** to protect the confidentiality and integrity of information on **[Assignment: organization-defined mobile devices]**. References: None.	
AC-21; ACCESS CONTROL; User-Based Collaboration And Information Sharing RENAMED: Information Sharing: The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for **[Assignment: organization-defined information sharing circumstances where user discretion is required]**; and b. Employs **[Assignment: organization-defined automated mechanisms or manual processes]** to assist users in making information sharing/collaboration decisions. References: None.	

AC-22; ACCESS CONTROL; Publicly Accessible Content: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information **[Assignment: organization-defined frequency]** and removes such information, if discovered. References: None.	AC-22 **Impact Levels 4-6:** d. Every 90 days or as new information is posted Source: DoD RMF TAG ---------- **Impact Level 2:** d. at least quarterly Source: FedRAMP v2 ----------
AC-23; ACCESS CONTROL; Data Mining Protection: The organization employs **[Assignment: organization-defined data mining prevention and detection techniques]** for **[Assignment: organization-defined data storage objects]** to adequately detect and protect against data mining. References: None.	
AT-1; AWARENESS AND TRAINING ; Security Awareness And Training Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy **[Assignment: organization-defined frequency];** and 2. Security awareness and training procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.	AT-1 **Impact Levels 4-6:** a. all personnel Source: DoD RMF TAG ---------- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ----------
AT-2; AWARENESS AND TRAINING; Security Awareness RENAMED: Security Awareness Training: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. **[Assignment: organization-defined frequency]** thereafter. References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publication 800-50.	AT-2 **All Impact Levels:** c. annually Source: DoD RMF TAG and FedRAMP v2 ----------

AT-3; AWARENESS AND TRAINING ; Security Training RENAMED: Role-based Security Training: The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. **[Assignment: organization-defined frequency]** thereafter. References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publications 800-16, 800-50.	AT-3 **All Impact Levels:** c. annually Source: DoD RMF TAG and FedRAMP v2 ----------
AT-3 (2); AWARENESS AND TRAINING ; Security Training RENAMED: Role-based Security Training - Enhancement: Physical Security Controls The organization provides **[Assignment: organization-defined personnel or roles]** with initial and **[Assignment: organization-defined frequency]** training in the employment and operation of physical security controls. References: None.	AT-3 (2) **Impact Levels 4-6:** all personnel with the assigned role of routine physical access to the space housing the infrastructure supporting the CSO and/or media containing customer's information Annual Source: DoD RMF TAG with adjustment for Commercial CSPs ----------
AT-3 (4); AWARENESS AND TRAINING; Role-based Security Training - Enhancement: Suspicious Communications And Anomalous System Behavior The organization provides training to its personnel on **[Assignment: organization-defined indicators of malicious code]** to recognize suspicious communications and anomalous behavior in organizational information systems. References: None.	
AT-4; AWARENESS AND TRAINING ; Security Training Records: The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for **[Assignment: organization-defined time period]**. References: None.	AT-4 **Impact Levels 4-6:** b. at least 5 years or 5 years after completion of a specific training program Source: DoD RMF TAG ---------- **Impact Level 2:** At least one year Source: FedRAMP v2 ----------

AU-1; AUDIT AND ACCOUNTABILITY; Audit And Accountability Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy **[Assignment: organization-defined frequency]**; and 2. Audit and accountability procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-100.	AU-1 **Impact Levels 4-6:** a. the ISSO and ISSM and others as the local organization deems appropriate b. 1. Annually Source: DoD RMF TAG ---------- **Impact Level 2:** b.1 at least every 3 years Source: FedRAMP v2 **All Impact Levels:** b.2 at least annually Source: DoD RMF TAG and FedRAMP v2 ----------
AU-2; AUDIT AND ACCOUNTABILITY; Auditable Events: The organization: a. Determines that the information system is capable of auditing the following events: **[Assignment: organization-defined auditable events]**; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: **[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]**. References: NIST Special Publication 800-92; Web: CSRC.NIST.GOV/PCIG/CIG.HTML, IDMANAGEMENT.GOV	AU-2 **Impact Levels 4-6:** a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart. d. all auditable events defined in AU-2 (a) per occurrence. Source: DoD RMF TAG ---------- **Impact Level 2:** a. Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; d. organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event. Source: FedRAMP v2 ----------
AU-2 (3); AUDIT AND ACCOUNTABILITY; Auditable Events - Enhancement: Reviews And Updates The organization reviews and updates the audited events **[Assignment: organization-defined frequency].** References: None.	AU-2 (3) **All Impact Levels:** Annually and based on situational awareness of threats, vulnerabilities Source: DoD RMF TAG and FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the Authorizing Official.

AU-3 (1); AUDIT AND ACCOUNTABILITY; Content Of Audit Records - Enhancement: Additional Audit Information The information system generates audit records containing the following **[Assignment: organization-defined additional, more detailed information]**. References: None.	AU-3 (1) **Impact Levels 4-6:** At a minimum, full-text recording of privileged commands or the individual identities of group account users. Source: DoD RMF TAG --- **Impact Level 2:** session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** AU-3 (1). Requirement: The service provider defines audit record types. The audit record types are approved and accepted by the Authorizing Official. Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.
AU-4; AUDIT AND ACCOUNTABILITY; Audit Storage Capacity: The organization allocates audit record storage capacity in accordance with **[Assignment: organization-defined audit record storage requirements]**. References: None.	
AU-4 (1); AUDIT AND ACCOUNTABILITY; Audit Storage Capacity - Enhancement: Transfer To Alternate Storage The information system off-loads audit records **[Assignment: organization-defined frequency]** onto a different system or media than the system being audited. References: None.	AU-4 (1) **Impact Levels 4-6:** At a minimum, real-time for interconnected systems and weekly for stand-alone systems Source: DoD RMF TAG ---
AU-5; AUDIT AND ACCOUNTABILITY; Response To Audit Processing Failures: The information system: a. Alerts **[Assignment: organization-defined personnel or roles]** in the event of an audit processing failure; and b. Takes the following additional actions: **[Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]**. References: None.	AU-5 **Impact Levels 4-6:** a. At a minimum, the SCA and ISSO Source: DoD RMF TAG --- **All Impact Levels :** b. low-impact: overwrite oldest audit records; moderate-impact: shut down Sourc: FedRAMP v2 ---

AU-6; AUDIT AND ACCOUNTABILITY; Audit Review, Analysis, And Reporting: The organization: a. Reviews and analyzes information system audit records **[Assignment: organization-defined frequency]** for indications of **[Assignment: organization-defined inappropriate or unusual activity]**; and b. Reports findings to **[Assignment: organization-defined personnel or roles]**. References: None.	AU-6 **Impact Levels 4-6:** a. every seven days or more frequently if required by an alarm event or anomaly; b. at a minimum, the ISSO and ISSM Source: DoD RMF TAG --- **Impact Level 2:** a. at least weekly Source: FedRAMP v2 ---
AU-7 (1); AUDIT AND ACCOUNTABILITY; Audit Reduction And Report Generation - Enhancement: Automatic Processing The information system provides the capability to process audit records for events of interest based on **[Assignment: organization-defined audit fields within audit records]**. References: None.	
AU-8; AUDIT AND ACCOUNTABILITY; Time Stamps: The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets **[Assignment: organization-defined granularity of time measurement]**. References: None.	AU-8 **Impact Levels 4-6:** b. one second Source: DoD RMF TAG ---
AU-8 (1); AUDIT AND ACCOUNTABILITY; Protection Of Audit Information - Enhancement: Synchronization With Authoritative Time Source The information system: a. Compares the internal information system clocks **[Assignment: organization-defined frequency]** with **[Assignment: organization-defined authoritative time source]** and; b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than **[Assignment: organization-defined time period].** References: None.	AU-8 (1) **Impact Levels 4-6:** a. an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS); b. Greater than the organizationally defined granularity in AU-8 Source: DoD RMF TAG --- **All Impact Levels:** a. At least hourly Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** AU-8 (1). Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server. Guidance: Synchronization of system clocks improves the accuracy of log analysis.

AU-9 (2); AUDIT AND ACCOUNTABILITY; Protection Of Audit Information - Enhancement: Audit Backup On Separate Physical Systems / Components The information system backs up audit records **[Assignment: organization-defined frequency]** onto a physically different system or system component than the system or component being audited. References: None.	AU-9 (2) **All Impact Levels:** at least weekly Source: DoD RMF TAG& FedRAMP v2 ----------
AU-9 (4); AUDIT AND ACCOUNTABILITY; Protection Of Audit Information - Enhancement: Access By Subset Of Privileged Users The organization authorizes access to management of audit functionality to only **[Assignment: organization-defined subset of privileged users].** References: None.	
AU-11; AUDIT AND ACCOUNTABILITY; Audit Record Retention: The organization retains audit records for **[Assignment: organization-defined time period consistent with records retention policy]** to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. References: None.	AU-11 **Impact Levels 4-6:** 5 years for SAMI; otherwise for at least 1 year Source: DoD RMF TAG ---------- **Impact Level 2:** at least ninety days Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** AU-11. Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements. NARA General Records Schedules http://www.archives.gov/records-mgmt/grs.html
AU-12; AUDIT AND ACCOUNTABILITY; Audit Generation: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at **[Assignment: organization-defined information system components];** b. Allows **[Assignment: organization-defined personnel or roles]** to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. References: None.	AU-12 **Impact Levels 4-6:** a. all information system and network components b. ISSM or individuals appointed by the ISSM Source: DoD RMF TAG ---------- **Impact Level 2:** a. all information system and network components where audit capability is deployed/available Source: FedRAMP v2 ----------

AU-12 (1); AUDIT AND ACCOUNTABILITY; Audit Generation - Enhancement: System-Wide / Time-Correlated Audit Trail The information system compiles audit records from **[Assignment: organization-defined information system components]** into a system-wide (logical or physical) audit trail that is time-correlated to within **[Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail]**. References: None.	AU-12 (1) **Impact Levels 4-6:** The time tracking tolerance defined in AU-8 Source: DoD RMF TAG ----------
CA-1; SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessment And Authorization Policies And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy **[Assignment: organization-defined frequency];** and 2. Security assessment and authorization procedures **[Assignment: organization-defined frequency].** References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.	CA-1 **Impact Levels 4-6:** a. all personnel Source: DoD RMF TAG ---------- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ----------
CA-2; SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation **[Assignment: organization-defined frequency]** to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to **[Assignment: organization-defined individuals or roles]**. References: Executive Order 12587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137	CA-2 **All Impact Levels:** b. at least annually Source: FedRAMP v2 ---------- d. at a minimum, the CSP's ISSO and ISSM, FedRAMP PMO (as applicable), the DISA A&A/SCA team, and the customer's MCD Source: FedRAMP v2, DoD RMF TAG with adjustment for Commercial and DoD private on-premises CSP/CSOs ----------

CA-2 (1); SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments - Enhancement: Independent Assessors The organization employs assessors or assessment teams with **[Assignment: organization-defined level of independence]** to conduct security control assessments. References: None.	CA-2 (1) **All Impact Levels:** Added to NIST Baseline for "Low" FedRAMP baseline. Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** For JAB Authorization, must be an accredited 3PAO
CA-2 (2); SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments - Enhancement: Specialized Assessments The organization includes as part of security control assessments, **[Assignment: organization-defined frequency],** **[Selection:** **- announced;** **- unannounced** **],** **[Selection (one or more):** **- in-depth monitoring;** **- vulnerability scanning;** **- malicious user testing;** **- insider threat assessment;** **- performance/load testing;** **- [Assignment: organization-defined other forms of security assessment]** **].** References: None.	CA-2 (2) **All Impact Levels:** at least annually Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Requirement: To include 'announced', 'vulnerability scanning'
CA-2 (3); SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments - Enhancement: External Organizations The organization accepts the results of an assessment of **[Assignment: organization-defined information system]** performed by **[Assignment: organization-defined external organization]** when the assessment meets **[Assignment: organization-defined requirements]**. References: None.	CA-2 (3) **All Impact Levels:** CSP and CSO infrastructure any FedRAMP Accredited 3PAO the conditions of a PA in the FedRAMP Repository Source: FedRAMP v2 ---
CA-3; SECURITY ASSESSMENT AND AUTHORIZATION; Information System Connections RENAMED: System Interconnections: The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements **[Assignment: organization-defined frequency]**. References: FIPS Publication 199; NIST Special Publication 800-47.	CA-3 **All Impact Levels:** c. at least annually Source: DoD RMF TAG --- **Impact Level 2:** c. 3 Years / Annually and on input from FedRAMP Source: FedRAMP v2 ---

CA-3 (1); SECURITY ASSESSMENT AND AUTHORIZATION; Information System Connections RENAMED: System Interconnections - Enhancement: Unclassified National Security System Connections The organization prohibits the direct connection of an **[Assignment: organization-defined unclassified, national security system]** to an external network without the use of **[Assignment: organization-defined boundary protection device]**. References: None.	CA-3 (1) **Impact Levels 4-6:** all unclassified NSS Source: DoD RMF TAG ----------
CA-3 (3); SECURITY ASSESSMENT AND AUTHORIZATION; System Interconnections - Enhancement: Unclassified Non-National Security System Connections The organization prohibits the direct connection of an **[Assignment: organization-defined unclassified, non-national security system]** to an external network without the use of **[Assignment; organization-defined boundary protection device]**. References: None.	CA-3 (3) **All Impact Levels:** Boundary Protections which meet the Trusted Internet Connection (TIC) requirements Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** CA-3(3) Guidance: Refer to Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document. https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
CA-3 (5); SECURITY ASSESSMENT AND AUTHORIZATION; System Interconnections - Enhancement: Restrictions On External System Connections The organization employs **[Selection:** **- allow-all,** **- deny-by-exception;** **- deny-all,** **- permit-by-exception** **]** policy for allowing **[Assignment: organization-defined information systems]** to connect to external information systems. References: None.	CA-3 (5) **Impact Levels 4-6:** deny-all, permit by exception any systems requiring external connectivity Source: DoD RMF TAG ---------- **All Impact Levels:** **FedRAMP Additional Requirements and Guidance:** For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing
CA-5; SECURITY ASSESSMENT AND AUTHORIZATION; Plan Of Action And Milestones: The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones **[Assignment: organization-defined frequency]** based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. References: OMB Memorandum 02-01; NIST Special Publication 800-37.	CA-5 **All Impact Levels:** b. at least monthly Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** CA-5 Guidance: Requirement: POA&Ms must be provided at least monthly.

CA-6; SECURITY ASSESSMENT AND AUTHORIZATION; Security Authorization: The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization **[Assignment: organization-defined frequency]**. References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publication 800-37, 800-137.	CA-6 **Impact Levels 4-6:** c. at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates. Source: DoD RMF TAG --- **Impact Level 2:** c. at least every three years or when a significant change occurs Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** CA-6c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the Authorizing Official.
CA-7; SECURITY ASSESSMENT AND AUTHORIZATION; Continuous Monitoring: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of **[Assignment: organization-defined metrics]** to be monitored; b. Establishment of **[Assignment: organization-defined frequencies]** for monitoring and **[Assignment: organization-defined frequencies]** for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to **[Assignment: organization-defined personnel or roles]** **[Assignment: organization-defined frequency].** References: OMG Memorandum 11-33; NIST Special Publications 800-37 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.	CA-7 **All Impact Levels:** d. To meet Federal and FedRAMP requirements Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Operating System Scans: at least monthly Database and Web Application Scans: at least monthly All scans performed by Independent Assessor: at least annually CA-7 Guidance: CSPs must provide evidence of closure and remediation of high vulnerabilities within the timeframe for standard POA&M updates NOTE: There is a discrepancy in the listing of ‘d’ in the parameter value, as ‘d’ does not have a parameter. This is however how the parameter is defined in FedRAMP v2.
CA-7 (1); SECURITY ASSESSMENT AND AUTHORIZATION; Continuous Monitoring - Enhancement: Independent Assessment The organization employs assessors or assessment teams with **[Assignment: organization-defined level of independence]** to monitor the security controls in the information system on an ongoing basis. References: None.	

CA-8; SECURITY ASSESSMENT AND AUTHORIZATION; Penetration Testing: The organization conducts penetration testing **[Assignment: organization-defined frequency]** on **[Assignment: organization-defined information systems or system components].** References: None.	CA-8 **All Impact Levels:** at least annually Source: FedRAMP v2 ----------
CA-9; SECURITY ASSESSMENT AND AUTHORIZATION; Internal System Connections: The organization: a. Authorizes internal connections of **[Assignment: organization-defined information system components or classes of components]** to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. References: None.	
CM-1; BASELINE CONFIGURATION; Configuration Management Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy **[Assignment: organization-defined frequency];** and 2. Configuration management procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-100.	CM-1 **Impact Levels 4-6:** a. all stakeholders in the configuration management process b.1. annually Source: DoD RMF TAG ---------- **Impact Level 2:** b.1. at least every 3 years **All Impact Levels:** b.2. at least annually Source: FedRAMP v2 ----------
CM-2 (1); BASELINE CONFIGURATION; Baseline Configuration - Enhancement: Reviews And Updates The organization reviews and updates the baseline configuration of the information system: (a) **[Assignment: organization-defined frequency];** (b) When required due to **[Assignment organization-defined circumstances]**; and (c) As an integral part of information system component installations and upgrades. References: None.	CM-2 (1) **All Impact Levels:** a. at least annually **Impact Levels 4-6:** b. baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber-attacks. Source: DoD RMF TAG ---------- **Impact Level 2:** b. to include when directed by Authorizing Official Source: FedRAMP v2 ----------

CM-2 (3); BASELINE CONFIGURATION; Baseline Configuration - Enhancement: Retention Of Previous Configurations The organization retains **[Assignment: organization-defined previous versions of baseline configurations of the information system]** to support rollback. References: None.	CM-2 (3) **Impact Levels 4-6:** the previous approved baseline configuration of IS components for a minimum of 3 month Source: DoD RMF TAG ----------
CM-2 (7); CONFIGURATION MANAGEMENT; Baseline Configuration - Enhancement: Configure Systems, Components, Or Devices For High-Risk Areas The organization: a. Issues **[Assignment: organization-defined information systems, system components, or devices]** with **[Assignment: organization-defined configurations]** to individuals traveling to locations that the organization deems to be of significant risk; and b. Applies **[Assignment: organization-defined security safeguards]** to the devices when the individuals return. References: None.	
CM-3; BASELINE CONFIGURATION; Configuration Change Control: The organization: a. Determines the type of changes to the information system that are configuration controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through **[Assignment: organization-defined configuration change control element (e.g., committee, board)]** that convenes **[Selection (one or more):** - **[Assignment: organization-defined frequency]**; - **[Assignment: organization-defined configuration change conditions]** **]**. References: NIST Special Publication 800-128.	CM-3 **Impact Levels 4-6:** e. The time period should be defined at the organization's CCB. g. a configuration control board; g. at a frequency determined by the CCB; g. configuration change conditions determined by the CCB. Source: DoD RMF TAG ---------- **All Impact Levels:** **FedRAMP Additional Requirements and Guidance:** Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the Authorizing Official. CM-3e Guidance: In accordance with record retention policies and procedures.
CM-3 (4); BASELINE CONFIGURATION; Configuration Change Control - Enhancement: Security Representative The organization requires an information security representative to be a member of the **[Assignment: organization-defined configuration change control element].** References: None.	CM-3 (4) **Impact Levels 4-6:** configuration control board (CCB) (as defined in CM-3, CCI 1586) Source: DoD RMF TAG ----------

CM-3 (6); CONFIGURATION MANAGEMENT; Configuration Change Control - Enhancement: Cryptography Management The organization ensures that cryptographic mechanisms used to provide **[Assignment: organization-defined security safeguards]** are under configuration management. References: None.	CM-3 (6) **Impact Levels 4-6:** All security safeguards that rely on cryptography Source: DoD RMF TAG & CNSSI 1253
CM-5 (3); BASELINE CONFIGURATION; Access Restrictions For Change - Enhancement: Signed Components The information system prevents the installation of **[Assignment: organization-defined critical software and firmware components]** without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. References: None.	CM-5 (3) **Impact Levels 4-6:** Any software or firmware components when the vendor provides digitally signed products Source: DoD RMF TAG --- **All Impact Levels:** **FedRAMP Additional Requirements and Guidance:** Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized.
CM-5 (5); BASELINE CONFIGURATION; Access Restrictions For Change - Enhancement: Limit Production / Operational Privileges The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges **[Assignment: organization-defined frequency]**. References: None.	CM-5 (5) **All Impact Levels:** b. at least quarterly Source: FedRAMP v2 ---
CM-6; BASELINE CONFIGURATION; Configuration Settings: The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using **[Assignment: organization-defined security configuration checklists]** that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for **[Assignment: organization-defined information system components]** based on **[Assignment: organization-defined operational requirements]**; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov; checklists.nist.gov; www.nsa.gov.	CM-6 **Impact Levels 4-6:** a. DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).; c. All configurable information system components; Source: DoD RMF TAG **NOTE**: DISA will evaluate Commercial CSP equivalencies on a case by case basis. --- **Impact Level 2:** a. See CM-6(a) Additional FedRAMP Requirements and Guidance Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** CM-6a. Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. CM-6a. Requirement: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). CM-6a. Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc .

CM-6 (1); BASELINE CONFIGURATION; Configuration Settings - Enhancement: Automated Central Management / Application / Verification The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for **[Assignment: organization-defined information system components]**. References: None.	
CM-7; BASELINE CONFIGURATION; Least Functionality: The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: **[Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services]**. References: DoD Instruction 8551.01	CM-7 **Impact Levels 4-6:** IAW DoDI 8551.01 Source: DoD RMF TAG --- **Impact Level 2:** United States Government Configuration Baseline (USGCB) Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. CM-7. Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc. (Partially derived from AC-17(8).)
CM-7 (1); BASELINE CONFIGURATION; Least Functionality - Enhancement: Periodic Review The organization: a. Reviews the information system **[Assignment: organization-defined frequency]** to identify unnecessary and/or non-secure functions, ports, protocols, and services; and b. Disables **[Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure]**. References: None.	CM-7 (1) **All Impact Levels:** a. at least monthly Source: FedRAMP v2 --- **Impact Levels 4-6:** b. Non-secure functions, ports, protocols and services are defined in DoDI 8551.01. Source: DoD RMF TAG ---
CM-7 (2); BASELINE CONFIGURATION; Least Functionality - Enhancement: Prevent Program Execution The information system prevents program execution in accordance with **[Selection (one or more):** **- [Assignment: organization-defined policies regarding software program usage and restrictions];** **- rules authorizing the terms and conditions of software program usage]**. References: None.	CM-7 (2) **All Impact Levels:** **FedRAMP Additional Requirements and Guidance:** CM-7(2) Guidance: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e. white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

CM-7 (5); CONFIGURATION MANAGEMENT; Least Functionality - Enhancement: Authorized Software / Whitelisting The organization: a. Identifies **[Assignment: organization-defined software programs authorized to execute on the information system]**; b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and c. Reviews and updates the list of authorized software programs **[Assignment: organization-defined frequency]**. References: None.	CM-7 (5) **Impact Levels 4-6:** c. Monthly Source: DoD RMF TAG --- **Impact Level 2:** c. at least Annually or when there is a change. Source: FedRAMP v2 ---
CM-8; BASELINE CONFIGURATION; Information System Component Inventory: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes **[Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]**; and b. Reviews and updates the information system component inventory **[Assignment: organization-defined frequency].** References: NIST Special Publication 800-128.	CM-8 **Impact Levels 4-6:** a. hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.; Source: DoD RMF TAG --- **All Impact Levels:** b. at least monthly Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** CM-8 Requirement: must be provided at least monthly or when there is a change.
CM-8 (3); BASELINE CONFIGURATION; Information System Component Inventory - Enhancement: Automated Unauthorized Component Detection The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: **[Selection (one or more):** **- disables network access by such components;** **- isolates the components;** **- notifies [Assignment: organization-defined personnel or roles]** **]**. References: None.	CM-8 (3) **Impact Levels 4-6:** b. the ISSO and ISSM and others as the local organization deems appropriate Source: DoD RMF TAG --- **All Impact Levels:** a. Continuously, using automated mechanisms with a maximum five-minute delay in detection. Source: FedRAMP v2 ---
CM-10 (1); CONFIGURATION MANAGEMENT; Software Usage Restrictions - Enhancement: Open Source Software The organization establishes the following restrictions on the use of open source software: **[Assignment: organization-defined restrictions].** References: None.	CM-10 (1) **Impact Levels 4-6:** IAW DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf). Source: DoD RMF TAG ---

CM-11; CONFIGURATION MANAGEMENT; User-Installed Software: The organization: a. Establishes **[Assignment: organization-defined policies]** governing the installation of software by users; b. Enforces software installation policies through **[Assignment: organization-defined methods]**; and c. Monitors policy compliance at **[Assignment: organization-defined frequency]**. References: None.	CM-11 **All Impact Levels:** c. Continuously (via CM-7 (5)) Source: FedRAMP v2 ----------
CP-1; CONTINGENCY PLANNING; Contingency Planning Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy **[Assignment: organization-defined frequency]**; and 2. Contingency planning procedures **[Assignment: organization-defined frequency].** References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.	CP-1 **Impact Levels 4-6:** a. all stakeholders identified in the contingency plan Source: DoD RMF TAG ---------- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ----------

CP-2; CONTINGENCY PLANNING; Contingency Plan: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by **[Assignment: organization-defined personnel or roles];** b. Distributes copies of the contingency plan to **[Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];** c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system **[Assignment: organization-defined frequency];** e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to **[Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]**; and g. Protects the contingency plan from unauthorized disclosure and modification. References: Federal Continuity Directive 1; NIST Special Publication 800-34.	CP-2 **Impact Levels 4-6:** a. at a minimum, the ISSM and ISSO b. all stakeholders identified in the contingency plan f: all stakeholders identified in the contingency plan Source: DoD RMF TAG --- **All Impact Levels:** d. at least annually Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.
CP-2 (3); CONTINGENCY PLANNING; Contingency Plan - Enhancement: Resume Essential Missions / Business Functions The organization plans for the resumption of essential missions and business functions within **[Assignment: organization-defined time period]** of contingency plan activation. References: None.	CP-2 (3) **Impact Levels 4-6:** 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan Source: DoD RMF TAG ---
CP-3; CONTINGENCY PLANNING; Contingency Training: The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within **[Assignment: organization-defined time period]** of assuming a contingency role or responsibility; b. When required by information system changes; and c. **[Assignment: organization-defined frequency]** thereafter. References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.	CP-3 **All Impact Levels:** a. 10 days c. at least annually Source: FedRAMP v2 ---

CP-4; CONTINGENCY PLANNING; Contingency Plan Testing And Exercises RENAMED: Contingency Plan Testing: The organization: a. Tests the contingency plan for the information system **[Assignment: organization-defined frequency]** using **[Assignment: organization-defined tests]** to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed. References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.	CP-4 **Impact Levels 4-6:** a. at least annually Source: DoD RMF TAG --- **Impact Level 2:** a. at least annually for moderate impact systems; at least every three years for low impact systems] [functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** a. Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by the Authorizing Official prior to initiating testing.
CP-7; CONTINGENCY PLANNING; Alternate Processing Site: The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of **[Assignment: organization-defined information system operations]** for essential missions/business functions within **[Assignment: organization-defined time period consistent with recovery time and recovery point objectives]** when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site. References: NIST Special Publication 800-34.	CP-7 **Impact Levels 4-6:** a. 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan Source: DoD RMF TAG --- **Impact Level 2:** **FedRAMP Additional Requirements and Guidance:** CP-7a. Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.
CP-8; CONTINGENCY PLANNING; Telecommunications Services: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of **[Assignment: organization-defined information system operations]** for essential missions and business functions within **[Assignment: organization-defined time period]** when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. References: NIST Special Publication 800-34; National Communications Directive 3-10; Web: TSP.NCS.GOV.	CP-8 **Impact Levels 4-6:** 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan Source: DoD RMF TAG --- **Impact Level 2:** **FedRAMP Additional Requirements and Guidance:** CP-8. Requirement: The service provider defines a time period consistent with the business impact analysis.

CP-9; CONTINGENCY PLANNING; Information System Backup: The organization: a. Conducts backups of user-level information contained in the information system **[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]**; b. Conducts backups of system-level information contained in the information system **[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]**; c. Conducts backups of information system documentation including security-related documentation **[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];** and d. Protects the confidentiality, integrity, and availability of backup information at the storage locations. References: NIST Special Publication 800-34.	CP-9 **Impact Levels 4-6:**c. when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan Source: DoD RMF TAG --- **All Impact Levels:** a. daily incremental; weekly full b. daily incremental; weekly full **Impact Level 2:** c. daily incremental; weekly full Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** CP-9. Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. Requirement: The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check. CP-9a. Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative. CP-9b. Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative. CP-9c. Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative.
CP-9 (1); CONTINGENCY PLANNING; Information System Backup - Enhancement: Testing For Reliability / Integrity The organization tests backup information **[Assignment: organization-defined frequency]** to verify media reliability and information integrity. References: None.	CP-9 (1) **Impact Levels 4-6:** at least monthly in accordance with contingency plan Source: DoD RMF TAG --- **Impact Level 2:**1. at least annually Source: FedRAMP v2 ---
CP-9 (3); CONTINGENCY PLANNING; Information System Backup - Enhancement: Separate Storage For Critical Information The organization stores backup copies of **[Assignment: organization-defined critical information system software and other security-related information]** in a separate facility or in a fire-rated container that is not collocated with the operational system. References: None.	

IA-1; IDENTIFICATION AND AUTHENTICATION; Identification And Authentication Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy **[Assignment: organization-defined frequency]**; 2. Identification and authentication procedures **[Assignment: organization-defined frequency].** References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.	IA-1 **Impact Levels 4-6:** the ISSO and ISSM and others as the local organization deems appropriate; b. 1. annually Source: DoD RMF TAG ---------- **Impact Level 2:** b.1 at least every 3 years **All Impact Levels:** b.2 at least annually Source: FedRAMP v2 ----------
IA-2 (11); IDENTIFICATION AND AUTHENTICATION; Identification And Authentication (Organizational Users) - Enhancement: Remote Access - Separate Device The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets **[Assignment: organization-defined strength of mechanism requirements].** References: None.	IA-2 (11) **Impact Levels 4-6:** DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval Source: DoD RMF TAG ----------
IA-3; IDENTIFICATION AND AUTHENTICATION; Device Identification And Authentication: The information system uniquely identifies and authenticates **[Assignment: organization-defined list of specific and/or types of devices]** before establishing a **[Selection (one or more):** **- local;** **- remote;** **- network** **]** connection. References: None.	IA-3 **Impact Levels 4-6:** all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs). Source: DoD RMF TAG ----------

IA-4; IDENTIFICATION AND AUTHENTICATION; Identifier Management: The organization manages information system identifiers by: a. Receiving authorization from **[Assignment: organization-defined personnel or roles]** to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for **[Assignment: organization-defined time period]**; and e. Disabling the identifier after **[Assignment: organization-defined time period of inactivity]**. References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.	IA-4 **Impact Levels 4-6:** a. ISSM or ISSO e. 35 days Source: DoD RMF TAG --- **All Impact Levels:** d. at least two years **Impact Level 2:** e. ninety days for user identifiers (See additional requirements and guidance.) Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** IA-4e. Requirement: The service provider defines time period of inactivity for device identifiers.
IA-4 (4); IDENTIFICATION AND AUTHENTICATION; Identifier Management - Enhancement: Identify User Status The organization manages individual identifiers by uniquely identifying each individual as **[Assignment: organization-defined characteristic identifying individual status]**. References: None.	IA-4 (4) **Impact Levels 4-6:** contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil Source: DoD RMF TAG --- **Impact Level 2:** contractors; foreign nationals Source: FedRAMP v2 ---

IA-5; IDENTIFICATION AND AUTHENTICATION; Authenticator Management: The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators **[Assignment: organization-defined time period by authenticator type]**; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes. References: OMB Memorandum 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov	IA-5 **Impact Levels 4-6:** g. CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: re-enroll every 3 years. Source: DoD RMF TAG ---------- **Impact Level 2:** g. to include sixty days for passwords Source: FedRAMP v2 ----------
IA-5 (1); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Password-Based Authentication The information system, for password-based authentication: (a) Enforces minimum password complexity of **[Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];** (b) Enforces at least the following number of changed characters when new passwords are created: **[Assignment: organization-defined number]**; (c) Stores and transmits only encrypted representations of passwords; (d) Enforces password minimum and maximum lifetime restrictions of **[Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]**; (e) Prohibits password reuse for **[Assignment: organization-defined number]** generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password. References: None.	IA-5 (1) **Impact Levels 4-6:** As supported by the device: a. minimum of 15 Characters, 1 of each of the following character sets: - Upper-case - Lower-case - Numeric - Special characters (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <)]; , Source: DoD RMF TAG ---------- **Impact Level 2:** Ia. case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters **All Impact Levels:** b. at least one d. one day minimum, sixty day maximum e. twenty four Source: FedRAMP v2 ----------

IA-5 (3); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: In-Person Or Trusted Third-Party Registration The organization requires that the registration process to receive **[Assignment: organization-defined types of and/or specific authenticators]** be conducted **[Selection:** **- in person;** **- by a trusted third party** **]** before **[Assignment: organization-defined registration authority]** with authorization by **[Assignment: organization-defined personnel or roles]**. References: None.	IA-5 (3) **Impact Levels 4-6:** The DoD PKI CP defines the role and responsibilities of a DoD PKI Registration Authority (RA). The NSS PKI CP defines the role and responsibilities of an NSS PKI RA. The DoD PKI RA–LRA CPS defines the nomination process for DoD PKI RAs. The NSS PKI DoD RPS defines the nomination process for NSS PKI RAs for DoD. The DoD PKI CP defines DoD PKI subscribers and the authentication requirements for issuance of credentials to subscribers. The NSS PKI CP defines NSS PKI subscribers and the authentication requirements for issuance of credentials to subscribers. Source: DoD RMF TAG ---------- **Impact Level 2:** All hardware/biometric (multifactor authenticators)in person Source: FedRAMP v2 ----------
IA-5 (4); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Automated Support For Password Strength Determination The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy **[Assignment: organization-defined requirements]**. References: None.	IA-5 (4) **Impact Levels 4-6:** complexity as identified in IA-5 (1) Part A Source: DoD RMF TAG ---------- **All Impact Levels:** **FedRAMP Additional Requirements and Guidance:** IA-4e Additional FedRAMP Requirements and Guidance: Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators
IA-5 (11); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Hardware Token-Based Authentication The information system, for hardware token-based authentication, employs mechanisms that satisfy **[Assignment: organization-defined token quality requirements]**. References: None.	IA-5 (11) **Impact Levels 4-6:** DoDI 8520.03 Source: DoD RMF TAG ----------
IA-5 (13); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Expiration Of Cached Authenticators The information system prohibits the use of cached authenticators after **[Assignment: organization-defined time period].** References: None.	

IA-8 (3); IDENTIFICATION AND AUTHENTICATION; Identification And Authentication (Non-Organization Users) - Enhancement: Use Of FICAM-Approved Products The organization employs only FICAM-approved information system components in **[Assignment: organization-defined information systems]** to accept third-party credentials. References: None.	
IR-1; INCIDENT RESPONSE; Incident Response Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy **[Assignment: organization-defined frequency]**; and 2. Incident response procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.	IR-1 **Impact Levels 4-6:** a. all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO Source: DoD RMF TAG --- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ---
IR-2; INCIDENT RESPONSE; Incident Response Training: The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within **[Assignment: organization-defined time period]** of assuming an incident response role or responsibility; b. When required by information system changes; and c. **[Assignment: organization-defined frequency]** thereafter. References: NIST Special Publications 800-16, 800-50.	IR-2 **Impact Levels 4-6:** a. 30 working days Source: DoD RMF TAG --- **All Impact Levels:** c. at least annually Source: FedRAMP v2 ---

IR-3; INCIDENT RESPONSE; Incident Response Testing And Exercises RENAMED: Incident Response Testing: The organization tests the incident response capability for the information system **[Assignment: organization-defined frequency]** using **[Assignment: organization-defined tests]** to determine the incident response effectiveness and documents the results. References: NIST Special Publications 800-84, 800-115.	IR-3 **Impact Levels 4-6:** At least every six months for high availability and at least annually for low/med availability Tests as defined in the incident response plan Source: DoD RMF TAG ---------- **Impact Level 2:** at least annually Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** IR-3. Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Requirement: For JAB Authorization, the service provider provides test plans to the Authorizing Official (AO) annually. Requirement: Test plans are approved and accepted by the Authorizing Official prior to test commencing.
IR-4 (3); INCIDENT RESPONSE; Incident Handling - Enhancement: Continuity Of Operations The organization identifies **[Assignment: organization-defined classes of incidents]** and **[Assignment: organization-defined actions to take in response to classes of incidents]** to ensure continuation of organizational missions and business functions. References: None.	IR-4 (3) **Impact Levels 4-6:** Classes of incidents defined in CJCSM 6510.01B Appendix A- Enclosure B Actions defined in CJCSM 6510.01B Source: DoD RMF TAG ----------
IR-4 (7); INCIDENT RESPONSE; Incident Handling - Enhancement: Insider Threats - Intra-Organization Coordination The organization coordinates incident handling capability for insider threats across **[Assignment: organization-defined components or elements of the organization]**. References: None.	
IR-4 (8); INCIDENT RESPONSE; Incident Handling - Enhancement: Correlation With External Organizations The organization coordinates with **[Assignment: organization-defined external organizations]** to correlate and share **[Assignment: organization-defined incident information]** to achieve a cross-organization perspective on incident awareness and more effective incident responses. References: None.	IR-4 (8) **Impact Levels 4-6:** The appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT), the Mission Owner's MCD, and Law Enforcement Incident information as defined in section 6.4 - Cyber Incident Reporting and Response Source: DoD RMF TAG with adjustment for Commercial CSPs ----------

IR-6; INCIDENT RESPONSE; Incident Reporting: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within **[Assignment: organization-defined time period]**; and b. Reports security incident information to **[Assignment: organization-defined authorities]**. References: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.	IR-6 **Impact Levels 4-6:** a. the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance b. The appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT), the Mission Owner's MCD, and Law Enforcement Source: DoD RMF TAG with adjustment for Commercial CSPs --- **Impact Level 2:** a. US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended) Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Requirement: Reports security incident information according to FedRAMP Incident Communications Procedure.
IR-6 (2); INCIDENT RESPONSE; Incident Reporting - Enhancement: Vulnerabilities Related To Incidents The organization reports information system vulnerabilities associated with reported security incidents to **[Assignment: organization-defined personnel or roles]**. References: None.	IR-6 (2)) **All Impact Levels:** the AOs who issued the PA and the customer's ATO, the customer's MCD, the CIRT/CERT (such as US-CERT, DoD CERT, IC CERT) Source: CC SRG best practice for community information sharing and mitigation of new vulnerabilities across the community

IR-8; INCIDENT RESPONSE; Incident Response Plan: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by **[Assignment: organization-defined personnel or roles]**; b. Distributes copies of the incident response plan to **[Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]**; c. Reviews the incident response plan **[Assignment: organization-defined frequency]**; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to **[Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]**; and f. Protects the incident response plan from unauthorized disclosure and modification. References: NIST Special Publication 800-61	IR-8 **Impact Levels 4-6:** a. at a minimum, the ISSM and ISSO b.all stakeholders identified in the incident response plan e. all stakeholders identified in the incident response plan, not later than 30 days after the change is made Source: DoD RMF TAG --- **All Impact Levels:** c. at least annually Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** IR-8(b) Additional FedRAMP Requirements and Guidance: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. IR-8(e) Additional FedRAMP Requirements and Guidance: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.
IR-9; INCIDENT RESPONSE; Information Spillage Response: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting **[Assignment: organization-defined personnel or roles]** of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other **[Assignment: organization-defined actions]**. References: None.	IR-9 **Impact Levels 4-6:** b. at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center Source: DoD RMF TAG --- f. time -sensitive actions that are necessary to limit the amount of damage or access. Keep a log of all actions taken regarding the CS/IA incident response, including the date/time of the action, who performed the action; create and maintain records, such as tickets, as appropriate for their role. Source: DoD Best Practice ---
IR-9 (1); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Responsible Personnel The organization assigns **[Assignment: organization-defined personnel or roles]** with responsibility for responding to information spills. References: None.	

IR-9 (2); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Training The organization provides information spillage response training **[Assignment: organization-defined frequency]**. References: None.	IR-9 (2) **Impact Levels 4-6:** Annually Source: DoD RMF TAG ----------
IR-9 (3); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Post-Spill Operations The organization implements **[Assignment: organization-defined procedures]** to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. References: None.	
IR-9 (4); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Exposure To Unauthorized Personnel The organization employs **[Assignment: organization-defined security safeguards]** for personnel exposed to information not within assigned access authorizations. References: None.	
MA-1; MAINTENANCE; System Maintenance Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy **[Assignment: organization-defined frequency]**; and 2. System maintenance procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-100.	MA-1 **Impact Levels 4-6:** a. all stakeholders identified in the maintenance policy Source: DoD RMF TAG ---------- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ----------

MA-2; MAINTENANCE; Controlled Maintenance: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that **[Assignment: organization-defined personnel or roles]** explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes **[Assignment: organization-defined maintenance-related information]** in organizational maintenance records. References: None.	
MA-3 (3); MAINTENANCE; Maintenance Tools - Enhancement: Prevent Unauthorized Removal The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from **[Assignment: organization-defined personnel or roles]** explicitly authorizing removal of the equipment from the facility. References: None.	MA-3 (3) **All Impact Levels:** d. the information owner explicitly authorizing removal of the equipment from the facility Source: FedRAMP v2 ----------
MA-6; MAINTENANCE; Timely Maintenance: The organization obtains maintenance support and/or spare parts for **[Assignment: organization-defined information system components]** within **[Assignment: organization-defined time period]** of failure. References: None.	MA-6 **Impact Levels 4-6:** **IAW CSO SLA or minimally as follows:** Within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability) Source: DoD RMF TAG ----------

MP-1; MEDIA PROTECTION; Media Protection Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy **[Assignment: organization-defined frequency]**; and 2. Media protection procedures **[Assignment: organization-defined frequency].** References: NIST Special Publications 800-12, 800-100.	MP-1 **Impact Levels 4-6:** a. all users Source: DoD RMF TAG --- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ---
MP-2; MEDIA PROTECTION; Media Access: The organization restricts access to **[Assignment: organization-defined types of digital and non-digital media]** to **[Assignment: organization-defined personnel or roles]**. References: FIPS Publication 199; NIST Special Publication 800-111	MP-2 **Impact Levels 4-6:** All types of digital and/or non-digital media containing information not cleared for public release Source: DoD RMF TAG ---
MP-3; MEDIA PROTECTION; Media Marking: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts **[Assignment: organization-defined types of information system media]** from marking as long as the media remain within **[Assignment: organization-defined controlled areas]**. References: FIPS Publication 199.	MP-3 **Impact Levels 4-6:** b. nothing unless otherwise exempted by DoDI 5200.01 and DoDM 5200.01 Vol 1-4 b. all areas unless otherwise exempted by DoDI 5200.01 and DoDM 5200.01 Vol 1-4 Source: DoD RMF TAG --- **Impact Level 2:** b. no removable media types Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** MP-3b. Guidance: Second parameter not-applicable

MP-4; MEDIA PROTECTION; Media Storage: The organization: a. Physically controls and securely stores **[Assignment: organization-defined types of digital and/or non-digital media]** within **[Assignment: organization-defined controlled areas]**; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-11	MP-4 **Impact Levels 4-6:** a 1. all digital and non-digital media containing sensitive, controlled, and/or classified information. a 2. areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media. Source: DoD RMF TAG --- **Impact Level 2:** a. all types of digital and non-digital media with sensitive information FedRAMP Assignment: see additional FedRAMP requirements and guidance Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** MP-4a Additional FedRAMP Requirements and Guidance: Requirement: The service provider defines controlled areas within facilities where the information and information system reside.
MP-5; MEDIA PROTECTION; Media Transport: The organization: a. Protects and controls **[Assignment: organization-defined types of information system media]** during transport outside of controlled areas using **[Assignment: organization-defined security safeguards]**; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with transport of information system media to authorized personnel. References: FIPS Publication 199; NIST Special Publication 800-60.	MP-5 **Impact Levels 4-6:** a. all digital and non-digital media containing sensitive, controlled, and/or classified information. a. DoDI 5200.1R and other organizationally defined security safeguards. Source: DoD RMF TAG and FedRAMP v2 --- **Impact Level 2:** a. all media with sensitive information prior to leaving secure/controlled environment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container Source: FedRAMP v2 ---
MP-6; MEDIA PROTECTION; Media Sanitization: The organization: a. Sanitizes **[Assignment: organization-defined information system media]** prior to disposal, release out of organizational control, or release for reuse using **[Assignment: organization-defined sanitization techniques and procedures]** in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.	MP-6 **Impact Levels 4-6:** a. all media a. techniques and procedures IAW NIST SP 800-88 and Section 5.9: Reuse and Disposal of Storage Media and Hardware. Source: DoD RMF TAG ---

MP-6 (2); MEDIA PROTECTION; Media Sanitization - Enhancement: Equipment Testing The organization tests sanitization equipment and procedures **[Assignment: organization-defined frequency]** to verify that the intended sanitization is being achieved. References: None.	MP-6 (2) **Impact Levels 4-6:** every 180 days. Source: DoD RMF TAG --- **Impact Level 2:** At least annually Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Guidance: Equipment and procedures may be tested or validated for effectiveness
MP-7; MEDIA PROTECTION; Media Use: The organization **[Selection: restricts; prohibits]** the use of **[Assignment: organization-defined types of information system media]** on **[Assignment: organization-defined information systems or system components]** using **[Assignment: organization-defined security safeguards].** References: FIPS Publication 199; NIST Special Publication 800-111.	
PE-1; PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical And Environmental Protection Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy **[Assignment: organization-defined frequency];** and 2. Physical and environmental protection procedures **[Assignment: organization-defined frequency].** References: NIST Special Publications 800-12, 800-100.	PE-1 **Impact Levels 4-6:** a. all personnel b.1 annually Source: DoD RMF TAG --- **Impact Level 2:** b.1 at least every 3 years **All Impact Levels:** b.2 at least annually Source: FedRAMP v2 ---
PE-2; PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical Access Authorizations: The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals **[Assignment: organization-defined frequency];** and d. Removes individuals from the facility access list when access is no longer required. References: None.	PE-2 **Impact Levels 4-6:** c. every 90 days Source: DoD RMF TAG --- **Impact Level 2:** c. at least annually Source: FedRAMP v2 ---

PE-3; PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical Access Control: The organization: a. Enforces physical access authorizations at **[Assignment: organization-defined entry/exit points to the facility where the information system resides]** by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using **[Selection (one or more):** **- [Assignment: organization-defined physical access control systems/devices];** **- guards** **]**; b. Maintains physical access audit logs for **[Assignment: organization-defined entry/exit points]**; c. Provides **[Assignment: organization-defined security safeguards]** to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity **[Assignment: organization-defined circumstances requiring visitor escorts and monitoring]**; e. Secures keys, combinations, and other physical access devices; f. Inventories **[Assignment: organization-defined physical access devices]** every **[Assignment: organization-defined frequency]**; and g. Changes combinations and keys **[Assignment: organization-defined frequency]** and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov	PE-3 **Impact Levels 4-6:** f. minimally keys or any other physical token used to gain access g. as required by security relevant events, at least annually Source: DoD RMF TAG and FedRAMP v2 ---------- **All Impact Levels:** a.2 CSP defined physical access control systems/devices AND guards d. in all circumstances within restricted access area where the information system resides f. at least annually g. at least annually Source: FedRAMP v2 ----------
PE-3 (1); PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical Access Control - Enhancement: Information System Access The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at **[Assignment: organization-defined physical spaces containing one or more components of the information system]**. References: None.	
PE-4; PHYSICAL AND ENVIRONMENTAL PROTECTION; Access Control For Transmission Medium: The organization controls physical access to **[Assignment: organization-defined information system distribution and transmission lines]** within organizational facilities using **[Assignment: organization-defined security safeguards]**. References: NSTISSI No. 7003.	

PE-6; PHYSICAL AND ENVIRONMENTAL PROTECTION; Monitoring Physical Access: The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs **[Assignment: organization-defined frequency]** and upon occurrence of **[Assignment: organization-defined events or potential indications of events]**; and c. Coordinates results of reviews and investigations with the organizational incident response capability. References: None.	PE-6 **All Impact Levels:** b.at least monthly Source: FedRAMP v2 ----------
PE-8; PHYSICAL AND ENVIRONMENTAL PROTECTION; Access Records RENAMED: Visitor Access Records: The organization: a. Maintains visitor access records to the facility where the information system resides for **[Assignment: organization-defined time period]**; and b. Reviews visitor access records **[Assignment: organization-defined frequency].** References: None.	PE-8 **All Impact Levels:** a for a minimum of one year b. at least monthly Source: FedRAMP v2 ----------
PE-10; PHYSICAL AND ENVIRONMENTAL PROTECTION; Emergency Shutoff: The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in **[Assignment: organization-defined location by information system or system component]** to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation. References: None.	
PE-13 (2); PHYSICAL AND ENVIRONMENTAL PROTECTION; Fire Protection - Enhancement: Suppression Devices / Systems The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to **[Assignment: organization-defined personnel or roles]** and **[Assignment: organization-defined emergency responders].** References: None.	

PE-14; PHYSICAL AND ENVIRONMENTAL PROTECTION; Temperature And Humidity Controls: The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at **[Assignment: organization-defined acceptable levels];** and b. Monitors temperature and humidity levels **[Assignment: organization-defined frequency].** References: None.	PE-14 **DoD CSPs:** NOTE: the DoD value shown for PE-14 is equivalent to the FedRAMP value and represents industry standards. It provides an evaluation benchmark. While this value is not appropriate for DoD to define for all CSP's infrastructure or service offerings, DoD CSPs must follow the DoD value while Commercial CSPs may use the FedRAMP value as follows: a. For commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; For other systems, levels within manufacturer specifications b. Continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required Source: DoD RMF TAG --- **Commercial CSPs:** a. consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments b. continuously Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** PE-14a. Requirements: The service provider measures temperature at server inlets and humidity levels by dew point.
PE-16; PHYSICAL AND ENVIRONMENTAL PROTECTION; Delivery And Removal: The organization authorizes, monitors, and controls **[Assignment: organization-defined types of information system components]** entering and exiting the facility and maintains records of those items. References: None.	PE-16 **All Impact Levels:** all information system components Source: FedRAMP v2 ---
PE-17; PHYSICAL AND ENVIRONMENTAL PROTECTION; Alternate Work Site: The organization: a. Employs **[Assignment: organization-defined security controls]** at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. References: NIST Special Publication 800-46.	

PL-1; PLANNING; Security Planning Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy **[Assignment: organization-defined frequency]**; and 2. Security planning procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-18, 800-100	PL-1 **Impact Levels 4-6:** a. all personnel Source: DoD RMF TAG --- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ---
PL-2; PLANNING; System Security Plan: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to **[Assignment: organization-defined personnel or roles]**; c. Reviews the security plan for the information system **[Assignment: organization-defined frequency];** d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification. References: NIST Special Publication 800-18.	PL-2 **Impact Levels 4-6:** b. at a minimum, the ISSO, ISSM and SCA Source: DoD RMF TAG --- **All Impact Levels:** c. [t least annually Source: FedRAMP v2 ---
PL-2 (3); PLANNING; System Security Plan - Enhancement: Plan / Coordinate With Other Organizational Entities The organization plans and coordinates security-related activities affecting the information system with **[Assignment: organization-defined individuals or groups]** before conducting such activities in order to reduce the impact on other organizational entities. References: None.	

PL-4; PLANNING; Rules Of Behavior: The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior **[Assignment: organization-defined frequency]**; and d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. References: NIST Publication 800-18.	PL-4 **Impact Levels 4-6:** c. annually Source: DoD RMF TAG ---------- **Impact Level 2:** c. At least every 3 years Source: FedRAMP v2 ----------
PL-8; PLANNING; Information Security Architecture: The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture **[Assignment: organization-defined frequency]** to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. References: None.	PL-8 **All Impact Levels:** b. At least annually Source: FedRAMP v2 ----------
PL-8 (1); PLANNING; Information Security Architecture - Enhancement: Defense-In-Depth The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates **[Assignment: organization-defined security safeguards]** to **[Assignment: organization-defined locations and architectural layers]**; and (b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner. References: None.	

PS-1; PERSONNEL SECURITY; Personnel Security Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy **[Assignment: organization-defined frequency];** and 2. Personnel security procedures **[Assignment: organization-defined frequency].** References: None.	PS-1 **Impact Levels 4-6:** a. all personnel Source: DoD RMF TAG --- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ---
PS-2; PERSONNEL SECURITY; Position Categorization RENAMED: Position Risk Designation: The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations **[Assignment: organization-defined frequency].** References: None.	PS-2 **Impact Levels 4-6:** c. Annually Source: DoD RMF TAG --- **Impact Level 2:** c. at least every three years Source: FedRAMP v2 ---
PS-3; PERSONNEL SECURITY; Personnel Screening: The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to **[Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].** References: None.	PS-3 **All Impact Levels:** b. for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions Source: FedRAMP v2 ---
PS-3 (3); PERSONNEL SECURITY; Personnel Screening - Enhancement: Information With Special Protection Measures The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: (a) Have valid access authorizations that are demonstrated by assigned official government duties; and (b) Satisfy **[Assignment: organization-defined additional personnel screening criteria].** References: None.	PS-3 (3) **All Impact Levels:** b. personnel screening criteria – as required by specific information Source: FedRAMP v2 ---

PS-4; PERSONNEL SECURITY; Personnel Termination: The organization, upon termination of individual employment: a. Disables information system access within **[Assignment: organization-defined time period]**; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of **[Assignment: organization-defined information security topics];** d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies **[Assignment: organization-defined personnel or roles]** within **[Assignment: organization-defined time period].** References: NIST Special Publication 800-35.	PS-4 **Impact Levels 4-6:** a. 8 hrs if unable to coordinate account deactivation with the time of termination. f. at a minimum, the ISSO and personnel responsible for revoking credentials f. immediately or within 24 hours Source: DoD RMF TAG (a. FedRAMP High Baseline WG) --- **Impact Level 2:** a. same day Source: FedRAMP v2 ---
PS-5; PERSONNEL SECURITY; Personnel Transfer: The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates **[Assignment: organization-defined transfer or reassignment actions]** within **[Assignment: organization-defined time period following the formal transfer action]**; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies **[Assignment: organization-defined personnel or roles]** within **[Assignment: organization-defined time period].** References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.	PS-5 **Impact Levels 4-6:** b. actions to ensure all system accesses no longer required are removed b. 24 hrs if unable to coordinate account deactivation with the time of transfer. d. at a minimum, the ISSO and personnel responsible for transferring credentials d. 24 hours Source: DoD RMF TAG (b. FedRAMP High Baseline WG) --- **Impact Level 2:** within 24 hours of the formal transfer action Source: FedRAMP v2 ---
PS-6; PERSONNEL SECURITY; Access Agreements: The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements **[Assignment: organization-defined frequency];** and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or **[Assignment: organization-defined frequency]**. References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web: idmanagement.gov.	PS-6 **Impact Levels 4-6:** c (2) when there is a change to the user's level of access, at least annually Source: DoD RMF TAG and FedRAMP v2 --- **All Impact Levels:** b. at least annually **Impact Level 2:** c.2. [at least annually] Source: FedRAMP v2 ---

PS-7; PERSONNEL SECURITY; Third-Party Personnel Security: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify **[Assignment: organization-defined personnel or roles]** of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within **[Assignment: organization-defined time period];** and e. Monitors provider compliance. References: None.	PS-7 **Impact Levels 4-6:** d. at a minimum, the ISSO and personnel responsible for transferring credentials d. 24 hrs if unable to coordinate account deactivation with the time of transfer or termination. Source: DoD RMF TAG (d. FedRAMP High Baseline WG) --- **Impact Level 2:** d. organization-defined time period – same day Source: FedRAMP v2 ---
PS-8; PERSONNEL SECURITY; Personnel Sanctions: The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies **[Assignment: organization-defined personnel or roles]** within **[Assignment: organization-defined time period]** when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. References: None.	PS-8 **Impact Levels 4-6:** b. at a minimum, the ISSO b. immediately Source: DoD RMF TAG ---
RA-1; RISK ASSESSMENT; Risk Assessment Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy **[Assignment: organization-defined frequency]**; and 2. Risk assessment procedures **[Assignment: organization-defined frequency]**. References: None.	RA-1 **Impact Levels 4-6:** a. at a minimum, the ISSM and ISSO Source: DoD RMF TAG --- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ---

RA-3; RISK ASSESSMENT; Risk Assessment: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in **[Selection:** **- security plan;** **- risk assessment report;** **- [Assignment: organization-defined document]** **];** c. Reviews risk assessment results **[Assignment: organization-defined frequency];** d. Disseminates risk assessment results to **[Assignment: organization-defined personnel or roles]**; and e. Updates the risk assessment **[Assignment: organization-defined frequency]** or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. References: None.	RA-3 **Impact Levels 4-6:** d. ISSM, ISSO, AO, and PM Source: DoD RMF TAG --- **All Impact Levels:** b. security assessment report c. at least every three years or when a significant change occurs e. at least every three years or when a significant change occurs Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. RA-3d. Requirement: to include the Authorizing Official; for JAB authorizations to include FedRAMP
RA-5; RISK ASSESSMENT; Vulnerability Scanning: The organization: a. Scans for vulnerabilities in the information system and hosted applications **[Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process]** and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities **[Assignment: organization-defined response times]** in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with **[Assignment: organization-defined personnel or roles]** to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). References: None.	RA-5 **Impact Levels 4-6:** a. every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs) d. IAW an authoritative source (e.g. IAVM, CTOs, DTMs) or high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate-risk vulnerabilities mitigated within ninety days from date of discovery e. at a minimum, the ISSM and ISSO Source: DoD RMF TAG and FedRAMP v2 --- **Impact Level 2:** a. monthly operating system/infrastructure; monthly web applications and databases d. high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate-risk vulnerabilities mitigated within ninety days from date of discovery Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** RA-5a. Requirement: an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually. RA-5e. Requirement: to include the Risk Executive; for JAB authorizations to include FedRAMP

RA-5 (2); RISK ASSESSMENT; Vulnerability Scanning - Enhancement: Update By Frequency / Prior To New Scan / When Identified The organization updates the information system vulnerabilities scanned **[Selection (one or more):** **- [Assignment: organization-defined frequency];** **- prior to a new scan;** **- when new vulnerabilities are identified and reported** **].** References: None.	RA-5 (2) **All Impact Levels:** prior to a new scan Source: FedRAMP v2 ----------
RA-5 (5); RISK ASSESSMENT; Vulnerability Scanning - Enhancement: Privileged Access The information system implements privileged access authorization to **[Assignment: organization-identified information system components]** for selected **[Assignment: organization-defined vulnerability scanning activities].** References: NIST Special Publication 800-65.	RA-5 (5) **Impact Levels 4-6:** all information systems and infrastructure components Source: DoD RMF TAG ---------- **Impact Level 2:** operating systems / web applications / databases all scans Source: FedRAMP v2 ----------
SA-1; SYSTEM AND SERVICES ACQUISITION; System And Services Acquisition Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy **[Assignment: organization-defined frequency];** and 2. System and services acquisition procedures **[Assignment: organization-defined frequency].** References: None.	SA-1 **Impact Levels 4-6:** a. all personnel Source: DoD RMF TAG ---------- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ----------
SA-3; SYSTEM AND SERVICES ACQUISITION; Life Cycle Support RENAMED: System Development Life Cycle: The organization: a. Manages the information system using **[Assignment: organization-defined system development life cycle]** that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities. References: None.	

SA-4 (2); SYSTEM AND SERVICES ACQUISITION; Acquisitions RENAMED: Acquisition Process - Enhancement: Design / Implementation Information For Security Controls The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: **[Selection (one or more):** **- security-relevant external system interfaces;** **- high-level design;** **- low-level design;** **- source code or hardware schematics;** **- [Assignment: organization-defined design/implementation information]** **]** at **[Assignment: organization-defined level of detail].** References: None.	SA-4 (2) **All Impact Levels:** to include security-relevant external system interfaces and high-level design Source: FedRAMP v2 ----------
SA-4 (8); SYSTEM AND SERVICES ACQUISITION; Acquisition Process - Enhancement: Continuous Monitoring Plan The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains **[Assignment: organization-defined level of detail].** References: None.	SA-4 (8) **All Impact Levels:** at least the minimum requirement as defined in control CA-7 Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** SA-4 (8) Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.
SA-5; SYSTEM AND SERVICES ACQUISITION; Information System Documentation: The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and **[Assignment: organization-defined actions]** in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to **[Assignment: organization-defined personnel or roles].** References: None.	SA-5 **Impact Levels 4-6:** e. at a minimum, the ISSO, ISSM, and SCA Source: DoD RMF TAG ----------

SA-9; SYSTEM AND SERVICES ACQUISITION; External Information System Services: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ **[Assignment: organization-defined security controls]** in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs **[Assignment: organization-defined processes, methods, and techniques]** to monitor security control compliance by external service providers on an ongoing basis. References: None.	SA-9 **Impact Levels 4-6:** a. security controls defined by CNSSI 1253 and FedRAMP Security Controls Baseline(s) Source: DoD RMF TAG and FedRAMP v2 --- **Impact Level 2:**a. FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system **All Impact Levels:** c. Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored Source: FedRAMP v2 ---
SA-9 (1); SYSTEM AND SERVICES ACQUISITION; External Information System Services - Enhancement: Risk Assessments / Organizational Approvals The organization: (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by **[Assignment: organization-defined personnel or roles]**. References: None.	SA-9 (1) **Impact Levels 4-6:** b. the DoD Component CIO or their delegate(s) Source: DoD RMF TAG --- **Impact Level 2:** see Additional Requirement and Guidance Source: FedRAMP v2 --- **FedRAMP Additional Requirements and Guidance:** SA-9 (1). Requirement: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. For JAB authorizations, future planned outsourced services are approved and accepted by the JAB.
SA-9 (2); SYSTEM AND SERVICES ACQUISITION; External Information Systems - Enhancement: Identification Of Functions / Ports / Protocols / Services The organization requires providers of **[Assignment: organization-defined external information system services]** to identify the functions, ports, protocols, and other services required for the use of such services. References: None.	SA-9 (2) **All Impact Levels:** All external systems where Federal information is processed, transmitted or stored Source: FedRAMP v2 ---
SA-9 (4); SYSTEM AND SERVICES ACQUISITION; External Information Systems - Enhancement: Consistent Interests Of Consumers And Providers The organization employs **[Assignment: organization-defined security safeguards]** to ensure that the interests of **[Assignment: organization-defined external service providers]** are consistent with and reflect organizational interests. References: None.	SA-9 (4) **All Impact Levels:** All external systems where Federal information is processed, transmitted or stored Source: FedRAMP v2 ---

SA-9 (5); SYSTEM AND SERVICES ACQUISITION; External Information Systems - Enhancement: Processing Storage And Service Location The organization restricts the location of **[Selection (one or more):** **- information processing;** **- information/data;** **- information system services** **]** to **[Assignment: organization-defined locations]** based on **[Assignment: organization-defined requirements or conditions].** References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org.	SA-9 (5) **All Impact Levels:** information processing, transmission, information data, AND information services Source: FedRAMP v2 ----------
SA-10; SYSTEM AND SERVICES ACQUISITION; Developer Configuration Management: The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service **[Selection (one or more):** **- design;** **- development;** **- implementation;** **- operation** **];** b. Document, manage, and control the integrity of changes to **[Assignment: organization-defined configuration items under configuration management]**; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to **[Assignment: organization-defined personnel].** References: None.	SA-10 **Impact Levels 4-6:** e. at a minimum, the ISSO and ISSM Source: DoD RMF TAG ---------- **All Impact Levels:** a. development, implementation, AND operation Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** SA-10e. Requirement: for JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.
SA-11; SYSTEM AND SERVICES ACQUISITION; Developer Security Testing RENAMED: Developer Security Testing And Evaluation: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform **[Selection (one or more):** **- unit;** **- integration;** **- system;** **- regression** **]** testing/evaluation at **[Assignment: organization-defined depth and coverage];** c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation. References: None.	SA-11 **All Impact Levels:** b. Unit, integration; system; regression the infrastructure level Source: DoD Best Practice ----------

SA-12; SYSTEM AND SERVICES ACQUISITION; Supply Chain Protection: The organization protects against supply chain threats to the information system, system component, or information system service by employing **[Assignment: organization-defined security safeguards]** as part of a comprehensive, defense-in-breadth information security strategy. References: None.	SA-12 **Impact Levels 5-6:** measures of protection IAW DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)" Source: DoD RMF TAG ----------
SA-19; SYSTEM AND SERVICES ACQUISITION; Component Authenticity: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and b. Reports counterfeit information system components to **[Selection (one or more):** **- source of counterfeit component;** **- [Assignment: organization-defined external reporting organizations];** **- [Assignment: organization-defined personnel or roles]** **].** References: None.	SA-19 **Impact Levels 5-6:** b. at a minimum, USCYBERCOM b. at a minimum, the ISSO, ISSM, and PM Source: DoD RMF TAG ----------
SC-1; SYSTEM AND COMMUNICATIONS PROTECTION; System And Communications Protection Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy **[Assignment: organization-defined frequency]**; and 2. System and communications protection procedures **[Assignment: organization-defined frequency]**. References: None.	SC-1 **Impact Levels 4-6:** a. at a minimum, the ISSM/ISSO Source: DoD RMF TAG ---------- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ----------
SC-5; SYSTEM AND COMMUNICATIONS PROTECTION; Denial Of Service Protection: The information system protects against or limits the effects of the following types of denial of service attacks: **[Assignment: organization-defined types of denial of service attacks or reference to source for such information]** by employing **[Assignment: organization-defined security safeguards]**. References: None.	

SC-6; SYSTEM AND COMMUNICATIONS PROTECTION; Resource Priority RENAMED: Resource Availability: The information system protects the availability of resources by allocating **[Assignment: organization-defined resources]** by **[Selection (one or more);** **- priority;** **- quota;** **- [Assignment: organization-defined security safeguards]** **].** References: None.	
SC-7 (4); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: External Telecommunications Services The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy **[Assignment: organization-defined frequency]** and removes exceptions that are no longer supported by an explicit mission/business need. References: None.	SC-7 (4) **Impact Levels 4-6:** e. every 180 days Source: DoD RMF TAG --- **Impact Level 2:** at least annually Source: FedRAMP v2 ---
SC-7 (8); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Route Traffic To Authenticated Proxy Servers The information system routes **[Assignment: organization-defined internal communications traffic]** to **[Assignment: organization-defined external networks]** through authenticated proxy servers at managed interfaces. References: None.	SC-7 (8) **Impact Levels 4-6:** protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP) any network external to the authorization boundary Source: DoD RMF TAG ---
SC-7 (11); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Restrict Incoming Communications Traffic The information system only allows incoming communications from **[Assignment: organization-defined authorized sources]** routed to **[Assignment: organization-defined authorized destinations]**. References: None.	

SC-7 (12); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Host-Based Protection The organization implements **[Assignment: organization-defined host-based boundary protection mechanisms]** at **[Assignment: organization-defined information system components].** References: None.	SC-7 (12) **Impact Levels 4-6:** Host Intrusion Prevention System (HIPS) All information system components. Source: DoD RMF TAG **NOTE**: DISA will evaluate Commercial CSP equivalencies on a case by case basis. ----------
SC-7 (13); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Isolation Of Security Tools / Mechanisms / Support Components The organization isolates **[Assignment: organization-defined information security tools, mechanisms, and support components]** from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system. References: None.	SC-7 (13) **Impact Levels 4-6:** key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, Cyber Defense Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. Source: DoD RMF TAG ---------- **Impact Level 2:** **FedRAMP Additional Requirements and Guidance:** SC-7 (13). Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.
SC-7 (14); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Protects Against Unauthorized Physical Connections The organization protects against unauthorized physical connections at **[Assignment: organization-defined managed interfaces].** References: None.	SC-7 (14) **Impact Levels 4-6:** internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. Source: DoD RMF TAG ----------
SC-8 (1); SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity - Enhancement: Cryptographic Or Alternate Physical Protection The information system implements cryptographic mechanisms to **[Selection (one or more):** **- prevent unauthorized disclosure of information;** **- detect changes to information** **]** during transmission unless otherwise protected by **[Assignment: organization-defined alternative physical safeguards].** References: None.	SC-8 (1) **All Impact Levels:** prevent unauthorized disclosure of information AND detect changes to information a hardened or alarmed carrier Protective Distribution System (PDS) Source: FedRAMP v2 ----------

SC-8 (2); SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity - Enhancement: Pre / Post Transmission Handling The information system maintains the **[Selection (one or more):** **- confidentiality;** **- integrity** **]** of information during preparation for transmission and during reception. References: None.	SC-8 (2); **Impact Levels 4-6:** Confidentiality and integrity Source: CNSSI 1253 ----------
SC-10; SYSTEM AND COMMUNICATIONS PROTECTION; Network Disconnect: The information system terminates the network connection associated with a communications session at the end of the session or after **[Assignment: organization-defined time period] of inactivity**. References: None.	SC-10 **Impact Levels 4-6:** 10 minutes privileged sessions and 15 minutes for user sessions Source: (FedRAMP High Baseline WG) ---------- **Impact Level 2:** no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions Source: FedRAMP v2 ----------
SC-12; SYSTEM AND COMMUNICATIONS PROTECTION; Cryptographic Key Establishment And Management: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with **[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]**. References: None.	SC-12 **Impact Levels 4-6:** DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems" Source: DoD RMF TAG ---------- **Impact Level 2:** **FedRAMP Additional Requirements and Guidance:** SC-12 Guidance: Federally approved cryptography
SC-12 (2); SYSTEM AND COMMUNICATIONS PROTECTION; Cryptographic Key Establishment And Management - Enhancement: Symmetric Keys The organization produces, controls, and distributes symmetric cryptographic keys using **[Selection:** **- NIST FIPS-compliant;** **- NSA-approved** **]** key management technology and processes. References: None.	SC-12 (2) **Impact Levels 4-6:** NIST Approved for Unclassified systems NSA Approved for Classified systems Source: DoD RMF TAG ---------- **Impact Levels 2:** NIST FIPS-compliant Source: FedRAMP v2 ----------

SC-13; SYSTEM AND COMMUNICATIONS PROTECTION; Use Of Cryptography RENAMED: Cryptographic Protection: The information system implements **[Assignment: organization-defined cryptographic uses and type of cryptography required for each use]** in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. References: None.	SC-13 **Impact Levels 4-6:** Protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography Source: DoD RMF TAG ---------- **Impact Level 2:** FIPS-validated or NSA-approved cryptography Source: FedRAMP v2 ----------
SC-15; SYSTEM AND COMMUNICATIONS PROTECTION; Collaborative Computing Devices: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: **[Assignment: organization-defined exceptions where remote activation is to be allowed]**; and b. Provides an explicit indication of use to users physically present at the devices. References: NIST Special Publication 800-28; DoD Instruction 8552.01	SC-15 **Impact Levels 4-6:** Dedicated VTC suites located in approved VTC locations that are centrally managed Source: DoD RMF TAG ---------- **Impact Level 2:** a. no exceptions Source: FedRAMP v2 ----------
SC-17; SYSTEM AND COMMUNICATIONS PROTECTION; Public Key Infrastructure Certificates: The organization issues public key certificates under an **[Assignment: organization-defined certificate policy]** or obtains public key certificates from an approved service provider. References: OMB Memorandum 08-23; NIST Special Publication 800-81	SC-17 **Impact Levels 4-6:** DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling." Source: DoD RMF TAG ----------
SC-23 (3); SYSTEM AND COMMUNICATIONS PROTECTION; Session Authenticity - Enhancement: Unique Session Identifiers With Randomization The information system generates a unique session identifier for each session with **[Assignment: organization-defined randomness requirements]** and recognizes only session identifiers that are system-generated. References: NIST Special Publications 800-56, 800-57, 800-111	
SC-23 (5); SYSTEM AND COMMUNICATIONS PROTECTION; Session Authenticity - Enhancement: Allowed Certificate Authorities The information system only allows the use of **[Assignment: organization-defined certificate authorities]** for verification of the establishment of protected sessions. References: None.	SC-23 (5) **Impact Levels 4-6:** DoD PKI established certificate authorities. Source: DoD RMF TAG ----------

SC-28; SYSTEM AND COMMUNICATIONS PROTECTION; Protection Of Information At Rest: The information system protects the **[Selection (one or more):** **- confidentiality;** **- integrity** **]** of **[Assignment: organization-defined information at rest].** References: None.	SC-28 **All Impact Levels:** confidentiality AND integrity Source: FedRAMP v2 ---------- **FedRAMP Additional Requirements and Guidance:** SC-28. Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.
SC-28 (1); SYSTEM AND COMMUNICATIONS PROTECTION; Protection Of Information At Rest - Enhancement: Cryptographic Protection The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of **[Assignment: organization-defined information]** on **[Assignment: organization-defined information system components].** References: None.	SC-28 (1) **Impact Levels 4-6:** any information system components storing data defined in SC-28 (1), 2473 Source: DoD RMF TAG ----------
SI-1; SYSTEM AND INFORMATION INTEGRITY; System And Information Integrity Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]:** 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy **[Assignment: organization-defined frequency];** and 2. System and information integrity procedures **[Assignment: organization-defined** frequency]. References: NIST Special Publication 800-83.	SI-1 **Impact Levels 4-6:** a. all appointed information assurance personnel Source: DoD RMF TAG ---------- **All Impact Levels:** b.1 at least every 3 years b.2 at least annually Source: FedRAMP v2 ----------
SI-2; SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation: The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within **[Assignment: organization-defined time period]** of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. References: None.	SI-2 **Impact Levels 4-6:** c. within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs) or within 30 days of release of updates Source: DoD RMF TAG and FedRAMP v2 ---------- **Impact Level 2:** c. Within 30 days of release of updates Source: FedRAMP v2 ----------

SI-2 (2); SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation - Enhancement: Automated Flaw Remediation Status The organization employs automated mechanisms **[Assignment: organization-defined frequency]** to determine the state of information system components with regard to flaw remediation. References: None.	SI-2 (2) **Impact Levels 4-6:** Continuously with host-based monitoring software. Annually for external scans by (Computer Network Defense Service Provider) CDSP Source: DoD RMF TAG ---------- **Impact Level 2:** at least monthly Source: FedRAMP v2 ----------
SI-2 (3); SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation - Enhancement: Time To Remediate Flaws / Benchmarks For Corrective Actions The organization: (a) Measures the time between flaw identification and flaw remediation; and (b) Establishes **[Assignment: organization-defined benchmarks]** for taking corrective actions. References: None.	SI-2 (3) **Impact Levels 4-6:** b. within the period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs) Source: DoD RMF TAG ----------
SI-2 (6); SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation - Enhancement: Removal Of Previous Versions Of Software / Firmware The organization removes **[Assignment: organization-defined software and firmware components]** after updated versions have been installed. References: None.	SI-2 (6) **Impact Levels 4-6:** All upgraded/replaced software and firmware components that are no longer required for operation Source: DoD RMF TAG ----------

SI-3; SYSTEM AND INFORMATION INTEGRITY; Malicious Code Protection: The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system **[Assignment: organization-defined frequency]** and real-time scans of files from external sources at **[Selection (one or more);** **- endpoint;** **- network entry/exit points** **]** as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. **[Selection (one or more):** **- block malicious code;** **- quarantine malicious code;** **- send alert to administrator;** **- [Assignment: organization-defined action]** **]** in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. References: None.	SI-3 **Impact Levels 4-6:** c (2). Block and quarantine malicious code and then send an alert to the administrator immediately (in real time) or in near real-time Source: DoD RMF TAG ---------- **All Impact Levels:** c.1 at least weekly to include endpoints **Impact Level 2:** c.2 to include alerting administrator or defined security personnel Source: FedRAMP v2 ----------
SI-3 (10); SYSTEM AND INFORMATION INTEGRITY; Malicious Code Protection - Enhancement: Malicious Code Analysis The organization: (a) Employs **[Assignment: organization-defined tools and techniques]** to analyze the characteristics and behavior of malicious code; and (b) Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes. References: None.	

SI-4; SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with **[Assignment: organization-defined monitoring objectives]**; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through **[Assignment: organization-defined techniques and methods]**; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides **[Assignment: organization-defined information system monitoring information]** to **[Assignment: organization-defined personnel or roles]** **[Selection (one or more):** **- as needed;** **- [Assignment: organization-defined frequency]** **].** References: None.	SI-4 **Impact Levels 4-6:** a. (1) sensor placement and monitoring requirements within CJCSI 6510.01F Source: DoD RMF TAG --- g. monitoring information related to a change in security posture and vulnerabilities that affects the DoD Mission Owner's system/application/information the AOs who issued the PA and the customer's ATO, and the DoD Mission Owner's MCD as needed. Source: CC SRG best practice for CSP integration with DoD processes ---
SI-4 (4); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Inbound And Outbound Communications Traffic The information system monitors inbound and outbound communications traffic **[Assignment: organization-defined frequency]** for unusual or unauthorized activities or conditions. References: None.	SI-4 (4) **All Impact Levels:** continually Source: FedRAMP v2 ---
SI-4 (5); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: System Generated Alerts The information system alerts **[Assignment: organization-defined personnel or roles]** when the following indications of compromise or potential compromise occur: **[Assignment: organization-defined compromise indicators].** References: None.	SI-4 (5) **Impact Levels 4-6:** at a minimum, the ISSM and ISSO Real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B Source: DoD RMF TAG --- **All Impact Levels:** **FedRAMP Additional Requirements and Guidance:** In accordance with the incident response plan.

SI-4 (12); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Automated Alerts The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: **[Assignment: organization-defined activities that trigger alerts].** References: None.	SI-4 (12) **Impact Levels 4-6:** When there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B Source: DoD RMF TAG ----------
SI-4 (19); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Individuals Posing Greater Risk The organization implements **[Assignment: organization-defined additional monitoring]** of individuals who have been identified by **[Assignment: organization-defined sources]** as posing an increased level of risk. References: None.	
SI-4 (20); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Privileged User The organization implements **[Assignment: organization-defined additional monitoring]** of privileged users. References: None.	
SI-4 (22); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Unauthorized Network Services The information system detects network services that have not been authorized or approved by **[Assignment: organization-defined authorization or approval processes]** and **[Selection (one or more):** **- audits;** **- alerts [Assignment: organization-defined personnel or roles]** **].** References: None.	SI-4 (22) **Impact Levels 4-6:** Alerts at a minimum, the ISSM or ISSO, and the Mission Owner's MCD Source: DoD RMF TAG with adjustment for Commercial CSPs ----------
SI-4 (23); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Host-Based Devices The organization implements **[Assignment: organization-defined host-based monitoring mechanisms]** at **[Assignment: organization-defined information system components]**. References: NIST Special Publications 800-147, 80-155.	SI-4 (23) **Impact Levels 4-6:** Host-based monitoring software all components Source: DoD RMF TAG ----------

SI-5; SYSTEM AND INFORMATION INTEGRITY; Security Alerts, Advisories, And Directives: The organization: a. Receives information system security alerts, advisories, and directives from **[Assignment: organization-defined external organizations]** on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: **[Selection (one or more):** **- [Assignment: organization-defined personnel or roles];** **- [Assignment: organization-defined elements within the organization];** **- [Assignment: organization-defined external organizations]** **];** and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. References: None.	SI-5 **Impact Levels 4-6:** a. At a minimum, USCYBERCOM. c. the ISSO and ISSM c. not applicable as elements are not selected as recipients of security alerts, advisories and directives c. CDSP Tier 1 for vetting. The CDSP Tier 1 will pass the information to the accredited Tier 2 CDSPs. Tier 2 CDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators) Source: DoD RMF TAG --- **Impact Level 2:** a. to include US-CERT c. to include system security personnel and administrators with configuration/patch-management responsibilities Source: FedRAMP v2 ---
SI-6; SYSTEM AND INFORMATION INTEGRITY; Security Functionality Verification: The information system: a. Verifies the correct operation of **[Assignment: organization-defined security functions]**; b. Performs this verification **[Selection (one or more):** **- [Assignment: organization-defined system transitional states];** **- upon command by user with appropriate privilege;** **- [Assignment: organization-defined frequency]** **];** c. Notifies **[Assignment: organization-defined personnel or roles]** of failed security verification tests; and d. **[Selection (one or more):** **- shuts the information system down;** **- restarts the information system;** **- [Assignment: organization-defined alternative action(s)]** **]** when anomalies are discovered. References: None.	SI-6 **All Impact Levels:** b to include upon system startup and/or restart at least monthly c to include system administrators and security personnel d to include notification of system administrators and security personnel Source: DoD RMF TAG and FedRAMP v2 ---
SI-7; SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring RENAMED: Software, Firmware, and Information Integrity: The organization employs integrity verification tools to detect unauthorized changes to **[Assignment: organization-defined software, firmware, and information].** References: None.	

SI-7 (1); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring RENAMED: Software, Firmware, And Information Integrity - Enhancement: Integrity Checks The information system performs an integrity check of **[Assignment: organization-defined software, firmware, and information]** **[Selection (one or more):** **- at startup;** **- at [Assignment: organization-defined transitional states or security-relevant events];** **- [Assignment: organization-defined frequency]** **]**. References: None.	SI-7 (1) **All Impact Levels:** Selection to include security relevant events and at least monthly Source: FedRAMP v2 ----------
SI-7 (7); SYSTEM AND INFORMATION INTEGRITY; Software, Firmware, And Information Integrity - Enhancement: Integration Of Detection And Response The organization incorporates the detection of unauthorized **[Assignment: organization-defined security-relevant changes to the information system]** into the organizational incident response capability. References: None.	
SI-10; SYSTEM AND INFORMATION INTEGRITY; Information Input Validation: The information system checks the validity of **[Assignment: organization-defined information inputs].** References: None.	SI-10 **Impact Levels 4-6:** All inputs except those identified specifically by the organization Source: DoD RMF TAG ----------
SI-11; SYSTEM AND INFORMATION INTEGRITY; Error Handling: The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to **[Assignment: organization-defined personnel or roles]**. References: None.	SI-11 **Impact Levels 4-6:** b. the ISSO, ISSM, and SCA Source: DoD RMF TAG ----------
SI-16; SYSTEM AND INFORMATION INTEGRITY; Memory Protection: The information system implements **[Assignment: organization-defined security safeguards]** to protect its memory from unauthorized code execution. References: None.	

Table 9 - Parameter Values for SLA controls/Enhancements Listed in Table 3

AC-2 (13); ACCESS CONTROL; Account Management - Enhancement: Disable Accounts For High-Risk Individuals The organization disables accounts of users posing a significant risk within **[Assignment: organization-defined time period]** of discovery of the risk. References: None.	AC-2 (13) **Impact Levels 4-6:** 30 minutes unless otherwise defined in formal organizational policy Source: DoD RMF TAG ----------
AC-3 (4); ACCESS CONTROL; Access Enforcement - Enhancement: Discretionary Access Control The information system enforces **[Assignment: organization-defined discretionary access control policies]** over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following: (a) Pass the information to any other subjects or objects; (b) Grant its privileges to other subjects; (c) Change security attributes on subjects, objects, the information system, or the information system's components; (d) Choose the security attributes to be associated with newly created or revised objects; or (e) Change the rules governing access control. References: None.	
AC-12 (1); ACCESS CONTROL; Session Termination - Enhancement: User-Initiated Logouts / Message Displays The information system: (a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to **[Assignment: organization-defined information resources]**; and (b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions. References: None.	AC-12 (1) **Impact Levels 5-6:** a. all Source: DoD RMF TAG ----------
AC-16; ACCESS CONTROL; Security Attributes: The organization: a. Provides the means to associate **[Assignment: organization-defined types of security attributes]** having **[Assignment: organization-defined security attribute values]** with information in storage, in process, and/or in transmission; b. Ensures that the security attribute associations are made and retained with the information; c. Establishes the permitted **[Assignment: organization-defined security attributes]** for **[Assignment: organization-defined information systems]**; and d. Determines the permitted **[Assignment: organization-defined values or ranges]** for each of the established security attributes. References: None.	AC-16 **Impact Levels 4-6:** c. security attributes defined in AC-16, CCIs 2256-2258 c. all information systems d. the values defined in AC-16, CCIs 2259-2261 Source: DoD RMF TAG ----------

AC-16 (6); ACCESS CONTROL; Security Attributes - Enhancement: Maintenance Of Attribute Association By Organization The organization allows personnel to associate, and maintain the association of **[Assignment: organization-defined security attributes]** with **[Assignment: organization-defined subjects and objects]** in accordance with **[Assignment: organization-defined security policies]**. References: None.	
AU-10; AUDIT AND ACCOUNTABILITY; Non-Repudiation: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed **[Assignment: organization-defined actions to be covered by non-repudiation].** References: None.	AU-10 **Impact Levels 5-6:** actions defined by DoDI 8520.02 and DoDI 8520.03 Source: DoD RMF TAG ----------
IA-3 (1); IDENTIFICATION AND AUTHENTICATION; Device Identification And Authentication - Enhancement: Cryptographic Bidirectional Authentication The information system authenticates **[Assignment: organization-defined specific devices and/or types of devices]** before establishing **[Selection (one or more):** **- local;** **- remote;** **- network** **]** connection using bidirectional authentication that is cryptographically based. References: None.	IA-3 (1) **Impact Levels 4-6:** Selection: Minimally remote and network DoD Supplemental guidance: Once a device is authentication it must be authorized using the principle of least privilege.
SC-7 (11); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Restrict Incoming Communications Traffic The information system only allows incoming communications from **[Assignment: organization-defined authorized sources]** routed to **[Assignment: organization-defined authorized destinations]**. References: None.	SC-7 (11) **Impact Level 4**
SC-7 (14); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Protects Against Unauthorized Physical Connections The organization protects against unauthorized physical connections at **[Assignment: organization-defined managed interfaces].** References: None.	SC-7 (14) **Impact Levels 4-5:** internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. Source: DoD RMF TAG ----------
SC-18 (3); SYSTEM AND COMMUNICATIONS PROTECTION; Mobile Code - Enhancement: Prevent Downloading / Execution The information system prevents the download and execution of **[Assignment: organization-defined unacceptable mobile code].** References: None.	SC-18 (3) **Impact Levels 5-6:** “All unacceptable mobile code such as: (a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the DoD CIO. (b) Unsigned Category 1 mobile code and Category 1 mobile code

	technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host). (d) Category 2 mobile code not obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate)." Source: CNSS 1253 Supplemental guidance: For the protection of the infrastructure supporting a CSO, CSPs should apply this control to their organizational IT systems and the infrastructure supporting their CSO(s) For the protection of Mission Owners', their end users, and networks; CSP CSOs must not support the downloading of mobile code which is deemed unacceptable to DoD. See Section 5.16: Mobile Code for more information.
SC-18 (4); SYSTEM AND COMMUNICATIONS PROTECTION; Mobile Code - Enhancement: Prevent Automatic Execution The information system prevents the automatic execution of mobile code in **[Assignment: organization-defined software applications]** and enforces **[Assignment: organization-defined actions]** prior to executing the code. References: NIST Special Publication 800-81	SC-18 (4) **Impact Levels 5-6:** Software applications and such as but not limited to email, scriptable document/file editing applications that support documents with embedded code (e.g., MS Office applications/documents), etc. Prompting the user for permission. Source: CNSS 1253, DoD RMF TAG with adjustment for Commercial CSPs

Appendix E Privacy Overlay Comparative C/CE Tables and Value Tables

This appendix provides tables containing C/CE that are in addition to, or modify, the FedRAMP and FedRAMP+ C/CE baselines. Additional tables are provided for the C/CE which have parameter values provided by the Privacy Overlay.

This section contains the following Tables:

- Table 10 - *FedRAMP M C/CE Modified or Required by Regulation*
- Table 11- *FedRAMP+ C/CE Modified or Required by Regulation*
- Table 12 - *Privacy Overlay C/CE Not Included In FedRAMP M* or FedRAMP+
- Table 13 - *PII/PHI Parameter Values for FedRAMP and FedRAMP+ C/CE*
- Table 14 - *PII/PHI Parameter Values for C/CE Not Included In FedRAMP M or FedRAMP+*

A future release of the CC SRG will contain additional information that will define which C/CE will need to be assessed for a Privacy Overlay Rider for a CSO's PA for those CSOs that are intended to handle PII or PHI. Mission Owner responsibilities will also be addressed.

The Privacy Overlay provides one or more codes in association with each C/CE addressed in the overlay to indicate how it is addressed in the overlay. These codes are as follows:

- A plus sign ("+") indicates the control should be selected.
- Two "dashes" ("--") indicates the control should not be selected. **
- The letter "E" indicates there is a control extension.
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter "V" indicates this overlay defines a value for an organizational-defined parameter for the control.
- The letter "R" indicates there is at least one regulatory/statutory reference that affects the control selection or that the control helps to meet the regulatory/statutory requirements.

** NOTE: there is only one CE, AC-2 (8) that has a code "--" which includes code "R" which means the CE must not be selected for regulatory reasons.

The tables begin on the next page.

Table 10 - FedRAMP M C/CE Modified or Required by Regulation

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
AC-01	FR.M	X	X	+GR	+GR	+GR	+ER
AC-02	FR.M	X	X	+EGVR	+EGVR	+EGVR	+EGR
AC-02 (09)	FR.M	X	X	GVR	GVR	GVR	R
AC-03	FR.M	X	X	+EGR	+EGR	+EGR	+GR
AC-04	FR.M	X	X		+GR	+GR	+R
AC-05	FR.M	X	X		+GR	+GR	+GR
AC-06	FR.M	X	X		+GR	+GR	+GR
AC-06 (01)	FR.M	X	X			+GR	+R
AC-06 (02)	FR.M	X	X		+GR	+GR	+R
AC-06 (05)	FR.M	X	X			+R	+R
AC-06 (09)	FR.M	X	X		+R	+R	+R
AC-06 (10)	FR.M	X	X		+R	+R	
AC-08	FR.M	X	X	GR	GR	GR	GR
AC-11	FR.M	X	X	+EVR	+EVR	+EVR	+GR
AC-14	FR.M	X	X		GR	GR	GR
AC-17	FR.M	X	X	+GR	+GR	+GR	+GR
AC-17 (01)	FR.M	X	X	+GR	+GR	+GR	+R
AC-17 (02)	FR.M	X	X	+R	+R	+R	+GR
AC-18 (01)	FR.M	X	X	+GR	+GR	+GR	
AC-19	FR.M	X	X	+ER	+ER	+ER	+GR
AC-19 (05)	FR.M	X	X	+EVR	+EVR	+EVR	+GVR
AC-20	FR.M	X	X	+EGR	+EGR	+EGR	+R
AC-20 (01)	FR.M	X	X	+R	+R	+R	+R
AC-21	FR.M	X	X	+GR	+GR	+GR	+GR
AC-22	FR.M	X	X	+GR	+GR	+GR	+R
AT-01	FR.M	X	X	+GR	+GR	+GR	+R
AT-02	FR.M	X	X	+ER	+ER	+ER	+GR
AT-03	FR.M	X	X	+ER	+ER	+ER	+R
AT-04	FR.M	X	X	+GR	+GR	+GR	+R
AU-01	FR.M	X	X	+GVR	+GVR	+GVR	+R
AU-02	FR.M	X	X	+GVR	+GVR	+GVR	+GR
AU-03	FR.M	X	X	+GR	+GR	+GR	+R
AU-04	FR.M	X	X		+GR	+GR	+R
AU-06	FR.M	X	X		+GR	+GR	+R
AU-06 (03)	FR.M	X	X		+R	+R	
AU-07	FR.M	X	X	+R	+R	+R	+R
AU-07 (01)	FR.M	X	X		+R	+R	+R
AU-09	FR.M	X	X	+GR	+GR	+GR	+R

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
AU-09 (04)	FR.M	X	X		GR	GR	
AU-12	FR.M	X	X		+R	+R	+R
CA-01	FR.M	X	X	+GR	+GR	+GR	+R
CA-02	FR.M	X	X	+GR	+GR	+GR	+VR
CA-03	FR.M	X	X		+R	+R	+GVR
CA-03 (03)	FR.M	X	X	+VR	+VR	+VR	+R
CA-03 (05)	FR.M	X	X	+VR	+VR	+VR	+R
CA-06	FR.M	X	X	+EGR	+EGR	+EGR	+GR
CA-07	FR.M	X	X		+GR	+GR	+GR
CA-08	FR.M	X	X			+GVR	
CA-09	FR.M	X	X		+GVR	+GVR	+VR
CM-04	FR.M	X	X	+GR	+GR	+GR	+R
CP-01	FR.M	X	X	+R	+R	+R	+R
CP-02	FR.M	X	X	+R	+R	+R	+GR
CP-07	FR.M	X	X		GR	GR	GVR
CP-09	FR.M	X	X		+ER	+ER	+ER
CP-10	FR.M	X	X		+R	+R	+R
IA-02	FR.M	X	X	+R	+R	+R	+R
IA-02 (11)	FR.M	X	X		+GR	+GR	
IA-04	FR.M	X	X	+ER	+ER	+ER	+GR
IA-05	FR.M	X	X		+R	+R	+GR
IA-07	FR.M	X	X	+GR	+GR	+GR	+GR
IA-08	FR.M	X	X		+R	+R	+R
IR-01	FR.M	X	X	+GVR	+GVR	+GVR	+GR
IR-02	FR.M	X	X	+GR	+GR	+GR	+GR
IR-04	FR.M	X	X	+GR	+GR	+GR	+GR
IR-05	FR.M	X	X	+GR	+GR	+GR	+R
IR-06	FR.M	X	X	+GVR	+GVR	+GVR	+R
IR-07	FR.M	X	X	+GR	+GR	+GR	+R
IR-08	FR.M	X	X	+GR	+GR	+GR	+GR
MA-01	FR.M	X	X		+ER	+ER	+GR
MA-05	FR.M	X	X	+GR	+GR	+GR	+GR
MP-01	FR.M	X	X	+VR	+VR	+VR	+VR
MP-02	FR.M	X	X	+VR	+VR	+VR	+VR
MP-03	FR.M	X	X	+GR	+GR	+GR	+GR
MP-04	FR.M	X	X	+VR	+VR	+VR	+R
MP-05	FR.M	X	X	+VR	+VR	+VR	+VR
MP-05 (04)	FR.M	X	X	+R	+R	+R	+GR
MP-06	FR.M	X	X		+GVR	+GVR	+VR

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
MP-07	FR.M	X	X		+GVR	+GVR	
MP-07 (01)	FR.M	X	X		+R	+R	
PE-02	FR.M	X	X	+R	+R	+R	+GR
PE-03	FR.M	X	X	+R	+R	+R	+R
PE-05	FR.M	X	X	+GR	+GR	+GR	+GR
PE-17	FR.M	X	X	+GR	+GR	+GR	
PL-02	FR.M	X	X	+EGR	+EGR	+EGR	+R
PL-04	FR.M	X	X	+EGR	+EGR	+EGR	
PL-08	FR.M	X	X	+GR	+GR	+GR	
PS-01	FR.M	X	X	+ER	+ER	+ER	+R
PS-02	FR.M	X	X	+ER	+ER	+ER	+GR
PS-03	FR.M	X	X	+ER	+ER	+ER	+GR
PS-03 (03)	FR.M	X	X	+GVR	+GVR	+GVR	+GR
PS-04	FR.M	X	X	+GR	+GR	+GR	+GR
PS-05	FR.M	X	X	+ER	+ER	+ER	+GR
PS-06	FR.M	X	X	+GR	+GR	+GR	+R
PS-07	FR.M	X	X	+GR	+GR	+GR	+R
PS-08	FR.M	X	X	+EGR	+EGR	+EGR	+R
RA-01	FR.M	X	X	+EGR	+EGR	+EGR	+R
RA-02	FR.M	X	X	+ER	+ER	+ER	+R
RA-03	FR.M	X	X	+EGVR	+EGVR	+EGVR	+GVR
SA-02	FR.M	X	X	+ER	+ER	+ER	
SA-03	FR.M	X	X	+GR	+GR	+GR	
SA-04	FR.M	X	X	+EGR	+EGR	+EGR	+ER
SA-08	FR.M	X	X	+GR	+GR	+GR	
SA-09 (05)	FR.M	X	X	+EGR	+EGR	+EGR	
SA-11	FR.M	X	X		+EGR	+EGR	
SC-02	FR.M	X	X		+ER	+ER	+ER
SC-04	FR.M	X	X	+GR	+GR	+GR	+R
SC-08	FR.M	X	X	+GVR	+GVR	+GVR	+VR
SC-08 (01)	FR.M	X	X	+EVR	+EVR	+EVR	+GR
SC-12	FR.M	X	X	+VR	+VR	+VR	+GR
SC-13	FR.M	X	X	+VR	+VR	+VR	+GR
SC-28	FR.M	X	X	+GVR	+GVR	+GVR	+R
SC-28 (01)	FR.M	X	X	+EGR	+EGR	+EGR	+GR
SI-01	FR.M	X	X	+R	+R	+R	+R
SI-04	FR.M	X	X	+GR	+GR	+GR	+R
SI-07	FR.M	X	X	+VR	+VR	+VR	+VR
SI-10	FR.M	X	X		+VR	+VR	

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
SI-11	FR.M	X	X	+VR	+VR	+VR	+VR
SI-12	FR.M	X	X	+EGR	+EGR	+EGR	+EGR

Table 11- FedRAMP+ C/CE Modified or Required by Regulation

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
AC-06 (07)	FR+	X	X	+VR	+VR	+VR	+VR
AC-23	FR+	X	X	EGR	EGR	EGR	
AU-04 (01)	FR+	X	X		GR	GR	R
AU-06 (10)	FR+	X	X		+GR	+GR	
CM-03 (06)	FR+	X	X	+GVR	+GVR	+GVR	+GVR
CM-04 (01)	FR+	X	X		+GR	+GR	
MA-04 (06)	FR+	X	X	+R	+R	+R	+R
SC-08 (02)	FR+		X		+GVR	+GVR	

Table 12 - Privacy Overlay C/CE Not Included In FedRAMP M or FedRAMP+

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
AC-02 (13)	SLA	X	X	+R	+R	+R	+R
AC-03 (09)	+	X	X		+EVR	+EVR	+R
AC-04 (08)	+	X	X			+VR	
AC-04 (15)	+	X	X		+GR	+GR	+R
AC-04 (17)	+	X	X		+GVR	+GVR	
AC-04 (18)	+	X	X		+GR	+GR	+R
AC-16	SLA	X	X	+GVR	+GVR	+GVR	+GVR
AC-16 (03)	+	X	X	+GVR	+GVR	+GVR	+GVR
AC-20 (03)	1253	X	X	+EGVR	+EGVR	+EGVR	
AU-07 (02)	+	X	X		+R	+R	+R
AU-09 (03)	+	X	X		+GR	+GR	+GR
AU-10	SLA/1253	X	X		+GR	+GR	+R
AU-10 (01)	+	X	X		+GR	+GR	+R
AU-12 (03)	1253	X	X		+VR	+VR	+VR
CA-09 (01)	+	X	X		+GR	+GR	+R
CM-04 (02)	+	X	X		+R	+R	+R
IA-02 (06)	+	X	X		+GR	+GR	
IA-02 (07)	+	X	X		+GR	+GR	
IA-04 (03)	+	X	X		+GR	+GR	
IR-10	1253	X	X	+GR	+GR	+GR	
MP-06 (01)	+	X	X	+GR	+GR	+GR	+GR
MP-06 (08)	+	X	X		+GR	+GR	
MP-08 (03)	+	X	X		+VR	+VR	+GVR
PE-18	+	X	X			+GR	+GR
PM-01	+	X	X	+GR	+GR	+GR	+R
PM-02	+	X	X	GR	GR	GR	+ER
PM-03	+	X	X	+R	+R	+R	
PM-05	+	X	X	+GR	+GR	+GR	+GR
PM-07	+	X	X	+GR	+GR	+GR	+R
PM-09	+	X	X	+ER	+ER	+ER	+ER
PM-10	+	X	X	+EGR	+EGR	+EGR	+ER
PM-11	+	X	X	+EGR	+EGR	+EGR	+R
PM-12	+	X	X	+ER	+ER	+ER	
PM-14	+	X	X	+EGR	+EGR	+EGR	
PM-15	+	X	X	+EGR	+EGR	+EGR	
PR; AP-01	+	X	X	+GR	+GR	+GR	
PR; AP-02	+	X	X	+GR	+GR	+GR	

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
PR; AR-01	+	X	X	+EGR	+EGR	+EGR	+GR
PR; AR-02	+	X	X	+GR	+GR	+GR	+R
PR; AR-03	+	X	X	+ER	+ER	+ER	+ER
PR; AR-04	+	X	X	+GVR	+GVR	+GVR	+R
PR; AR-05	+	X	X	+EGR	+EGR	+EGR	+R
PR; AR-06	+	X	X	+R	+R	+R	+GR
PR; AR-07	+	X	X	+GR	+GR	+GR	+R
PR; AR-08	+	X	X	+R	+R	+R	+GR
PR; DI-01	+	X	X	+GR	+GR	+GR	
PR; DI-01 (01)	+	X	X		+GR	+GR	
PR; DI-01 (02)	+	X	X		+VR	+VR	
PR; DM-01	+	X	X	+GR	+GR	+GR	+R
PR; DM-02	+	X	X	+VR	+VR	+VR	+VR
PR; DM-03	+	X	X	+GR	+GR	+GR	+GR
PR; DM-03 (01)	+	X	X	GR	GR	GR	+GR
PR; IP-01	+	X	X	+GR	+GR	+GR	+GR
PR; IP-02	+	X	X	+GR	+GR	+GR	+ER
PR; IP-03	+	X	X	+GR	+GR	+GR	+R
PR; IP-04	+	X	X	+R	+R	+R	+R
PR; IP-04 (01)	+	X	X	GR	GR	GR	+R
PR; SE-01	+	X	X	+GR	+GR	+GR	+R
PR; SE-02	+	X	X	+GR	+GR	+GR	+R
PR; TR-01	+	X	X	+GR	+GR	+GR	+GR
PR; TR-02	+	X	X	+GR	+GR	+GR	
PR; TR-02 (01)	+	X	X	+GR	+GR	+GR	
PR; TR-03	+	X	X	+R	+R	+R	
PR; UL-01	+	X	X	+EGR	+EGR	+EGR	+R
PR; UL-02	+	X	X	+EGR	+EGR	+EGR	+GR
SA-11 (05)	+	X	X			+ER	
SA-15 (09)	1253	X	X		+EGR	+EGR	
SA-17	+	X	X	+EGR	+EGR	+EGR	
SA-21	+	X	X	+GVR	+GVR	+GVR	+GR
SC-08 (02)	1253	X			+GVR	+GVR	
SI-07 (06)	+	X	X	+ER	+ER	+ER	+GR

Table 13 - PII/PHI Parameter Values for FedRAMP and FedRAMP+ C/CE

Note: This table may modify the parameter values in Table 8 and Table 9 when PII/PHI are involved.

AC-2; ACCESS CONTROL; Account Management: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: **[Assignment: organization-defined information system account types]**; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by **[Assignment: organization-defined personnel or roles]** for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with **[Assignment: organization-defined procedures or conditions]**; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements **[Assignment: organization-defined frequency]**; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. References: None.	Low and Moderate PII Confidentiality Impact Level Parameter Value: f.… the requirement for each user to complete annual privacy training, or otherwise the account would be disabled. j.… at least annually. Source: CNSSI 1253 Privacy Overlay
AC-2 (9); ACCESS CONTROL; Account Management - Enhancement: Restrictions On Use Of Shared Groups / Accounts The organization only permits the use of shared/group accounts that meet **[Assignment: organization-defined conditions for establishing shared/group accounts].** References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … the requirement to uniquely attribute user activity to an account.…… . Source: CNSSI 1253 Privacy Overlay
AC-6 (7); ACCESS CONTROL; Least Privilege - Enhancement: Review Of User Privileges The organization: (a) Reviews **[Assignment: organization-defined frequency]** the privileges assigned to **[Assignment: organization-defined roles or classes of users]** to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs. References: None.	Low and Moderate PII Confidentiality Impact Level Parameter Value: (a) … at least annually… … individuals with access to low or moderate confidentiality impact level PII…… PHI Parameter Value: (a) … at least quarterly… …… individuals with access to privileged accounts… AND (a) … at least annually… … individuals with access to PHI…… Source: CNSSI 1253 Privacy Overlay

AC-11; ACCESS CONTROL; Session Lock: The information system: a. Prevents further access to the system by initiating a session lock after **[Assignment: organization-defined time period]** of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. References: OMB Memorandum 06-16.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: a. … no more than 30 minutes… Source: CNSSI 1253 Privacy Overlay
AC-19 (5); ACCESS CONTROL; Access Control For Mobile Devices - Enhancement: Full Device / Container- Based Encryption The organization employs **[Selection:** **- full-device encryption;** **- container encryption** **]** to protect the confidentiality and integrity of information on **[Assignment: organization-defined mobile devices]**. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … full-device encryption or container encryption… … on any type of mobile device permitted by the organization to access PII… PHI Parameter Value: … full device encryption or container encryption… … on any type of mobile device permitted by the organization to access PHI… Source: CNSSI 1253 Privacy Overlay
AU-1; AUDIT AND ACCOUNTABILITY; Audit And Accountability Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy **[Assignment: organization-defined frequency]**; and 2. Audit and accountability procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-100.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: b.1. … in accordance with organizational policy but not less than annually… Source: CNSSI 1253 Privacy Overlay
AU-2; AUDIT AND ACCOUNTABILITY; Auditable Events: The organization: a. Determines that the information system is capable of auditing the following events: **[Assignment: organization-defined auditable events]**; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: **[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]**. References: NIST Special Publication 800-92; Web: CSRC.NIST.GOV/PCIG/CIG.HTML, IDMANAGEMENT.GOV	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: a. … monitor system access, including unsuccessful and successful login attempts, to information systems containing PII… … successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository… … privileged activities or system level access to PII… … concurrent logons from different workstations… … all program, e.g., executable file, initiations… d. … monitor system access, including unsuccessful and successful login attempts, to information systems containing PII… … successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository… … privileged activities or system level access to PII… … concurrent logons from different workstations… … all program, e.g., executable file, initiations… Source: CNSSI 1253 Privacy Overlay

CA-3 (3); SECURITY ASSESSMENT AND AUTHORIZATION; System Interconnections - Enhancement: Unclassified Non-National Security System Connections The organization prohibits the direct connection of an **[Assignment: organization-defined unclassified, non-national security system]** to an external network without the use of **[Assignment; organization-defined boundary protection device]**. References: None.	Low, Moderate and High PII Confidentiality Impact Level Parameter Value: … systems containing PII… … a firewall or other network boundary protection device approved to prevent unauthorized access to the system… Source: CNSSI 1253 Privacy Overlay
CA-3 (5); SECURITY ASSESSMENT AND AUTHORIZATION; System Interconnections - Enhancement: Restrictions On External System Connections The organization employs **[Selection:** **- allow-all,** **- deny-by-exception;** **- deny-all,** **- permit-by-exception** **]** policy for allowing **[Assignment: organization-defined information systems]** to connect to external information systems. References: None.	Low, Moderate and High PII Confidentiality Impact Level Parameter Value: … permit-by-exception… … information systems containing PII… Source: CNSSI 1253 Privacy Overlay
CA-8; SECURITY ASSESSMENT AND AUTHORIZATION; Penetration Testing: The organization conducts penetration testing **[Assignment: organization-defined frequency]** on **[Assignment: organization-defined information systems or system components].** References: None.	High PII Confidentiality Impact Level Parameter Value: … prior to authorization of information system and periodically no less frequently than when a significant change to the information system occurs… … information systems containing PII at the High PII confidentiality impact level… Source: CNSSI 1253 Privacy Overlay
CA-9; SECURITY ASSESSMENT AND AUTHORIZATION; Internal System Connections: The organization: a. Authorizes internal connections of **[Assignment: organization-defined information system components or classes of components]** to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Value: … information systems containing PII… PHI Parameter Value: … information systems containing PHI… Source: CNSSI 1253 Privacy Overlay
CM-3 (6); CONFIGURATION MANAGEMENT; Configuration Change Control - Enhancement: Cryptography Management The organization ensures that cryptographic mechanisms used to provide **[Assignment: organization-defined security safeguards]** are under configuration management. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … … encryption of Low, Moderate, and High PII…… PHI Parameter Value: … encryption of PHI… Source: CNSSI 1253 Privacy Overlay

IR-1; INCIDENT RESPONSE; Incident Response Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy **[Assignment: organization-defined frequency]**; and 2. Incident response procedures **[Assignment: organization-defined frequency]**. References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: a. … Incident Response Team as required by OMB M-07-16… Source: CNSSI 1253 Privacy Overlay
IR-6; INCIDENT RESPONSE; Incident Reporting: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within **[Assignment: organization-defined time period]**; and b. Reports security incident information to **[Assignment: organization-defined authorities]**. References: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: a. … as short a time as is possible, but in no case later than one hour, after discovery or detection for incidents involving PII… b. … both the Privacy Incident Response Team and the appropriate incident response center, e.g., US-CERT or IC SCC, if the incident involves PII… Source: CNSSI 1253 Privacy Overlay
MP-1; MEDIA PROTECTION; Media Protection Policy And Procedures: The organization: a. Develops, documents, and disseminates to **[Assignment: organization-defined personnel or roles]**: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy **[Assignment: organization-defined frequency]**; and 2. Media protection procedures **[Assignment: organization-defined frequency].** References: NIST Special Publications 800-12, 800-100.	Low, Moderate and High PII Confidentiality Impact Level Parameter Value: a. … employees and contractors with potential access to PII…… PHI Parameter Value: a. … employees and contractors with potential access to PHI… Source: CNSSI 1253 Privacy Overlay …
MP-2; MEDIA PROTECTION; Media Access: The organization restricts access to **[Assignment: organization-defined types of digital and non-digital media]** to **[Assignment: organization-defined personnel or roles]**. References: FIPS Publication 199; NIST Special Publication 800-111	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … any digital or non-digital media containing PII…… … authorized individuals with a valid need to know… PHI Parameter Values: … any digital or non-digital media containing PHI…… … authorized individuals with a valid need to know…

MP-4; MEDIA PROTECTION; Media Storage: The organization: a. Physically controls and securely stores **[Assignment: organization-defined types of digital and/or non-digital media]** within **[Assignment: organization-defined controlled areas]**; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-11	Low, Moderate and High PII Confidentiality Impact Level Parameter Value: a. … removable media that contains PII…… … any securable area or in a locked container…… Source: CNSSI 1253 Privacy Overlay
MP-5; MEDIA PROTECTION; Media Transport: The organization: a. Protects and controls **[Assignment: organization-defined types of information system media]** during transport outside of controlled areas using **[Assignment: organization-defined security safeguards]**; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with transport of information system media to authorized personnel. References: FIPS Publication 199; NIST Special Publication 800-60.	Low, Moderate and High PII Confidentiality Impact Level Parameter Value: a. … digital media that contains PII…… … NSA-approved or FIPS-validated encryption… PHI Parameter Value: a. … digital media that contains PHI…… … NSA-approved or FIPS-validated encryption… Source: CNSSI 1253 Privacy Overlay
MP-6; MEDIA PROTECTION; Media Sanitization: The organization: a. Sanitizes **[Assignment: organization-defined information system media]** prior to disposal, release out of organizational control, or release for reuse using **[Assignment: organization-defined sanitization techniques and procedures]** in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.	Moderate and High PII Confidentiality Impact Level Parameter Value: a. … digital media that contains PII…… … NSA-approved or FIPS-validated media sanitization techniques or procedures… PHI Parameter Value: a. … digital media that contains PHI…… … NSA-approved or FIPS-validated media sanitization techniques or procedures… Source: CNSSI 1253 Privacy Overlay
MP-7; MEDIA PROTECTION; Media Use: The organization **[Selection:** **restricts;** **prohibits** **] .** the use of **[Assignment: organization-defined types of information system media]** on **[Assignment: organization-defined information systems or system components]** using **[Assignment: organization-defined security safeguards].** References: FIPS Publication 199; NIST Special Publication 800-111.	Moderate and High PII Confidentiality Impact Level Parameter Value: … restricts… … portable storage and mobile devices… … information systems and networks containing PII, without… … device ownership, media sanitization and encryption controls… Source: CNSSI 1253 Privacy Overlay

PS-3 (3); PERSONNEL SECURITY; Personnel Screening - Enhancement: Information With Special Protection Measures The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: (a) Have valid access authorizations that are demonstrated by assigned official government duties; and (b) Satisfy **[Assignment: organization-defined additional personnel screening criteria].** References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … organization defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII … Source: CNSSI 1253 Privacy Overlay
RA-3; RISK ASSESSMENT; Risk Assessment: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in **[Selection:** **- security plan;** **- risk assessment report;** **- [Assignment: organization-defined document]** **];** c. Reviews risk assessment results **[Assignment: organization-defined frequency];** d. Disseminates risk assessment results to **[Assignment: organization-defined personnel or roles]**; and e. Updates the risk assessment **[Assignment: organization-defined frequency]** or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: b. … an evaluation of risks associated with the potential impact of loss of the PII must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings… PHI Parameter Values: b. … a HIPAA Risk Analysis, and associated risks to PHI must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings. All HIPAA Risk Analysis documentation must be maintained for 6 years from the date of creation or date it was last in effect – whichever is later… Source: CNSSI 1253 Privacy Overlay
SC-8; SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity: The information system protects the **[Selection (one or more):** **- confidentiality;** **- integrity** **]** of transmitted information. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … confidentiality and integrity… PHI Parameter Values: … confidentiality and integrity… Source: CNSSI 1253 Privacy Overlay
SC-8 (1); SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity - Enhancement: Cryptographic Or Alternate Physical Protection The information system implements cryptographic mechanisms to **[Selection (one or more):** **- prevent unauthorized disclosure of information;** **- detect changes to information** **]** during transmission unless otherwise protected by **[Assignment: organization-defined alternative physical safeguards].** References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … prevent unauthorized disclosure of PII… … physical safeguard measures to prevent unauthorized access to or alteration of the PII contained therein…… Source: CNSSI 1253 Privacy Overlay

SC-8 (2); SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity - Enhancement: Pre / Post Transmission Handling The information system maintains the **[Selection (one or more):** **- confidentiality;** **- integrity** **]** of information during preparation for transmission and during reception. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Values: … confidentiality and integrity… Source: CNSSI 1253 Privacy Overlay
SC-12; SYSTEM AND COMMUNICATIONS PROTECTION; Cryptographic Key Establishment And Management: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with **[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]**. References: None.	Low, Moderate, High PII Confidentiality Impact Level Parameter Values: …centralized management of key generation, distribution, storage, access, and destruction in accordance with NIST SP 800-55 and NIST SP 800-57… Source: CNSSI 1253 Privacy Overlay
SC-13; SYSTEM AND COMMUNICATIONS PROTECTION; Use Of Cryptography RENAMED: Cryptographic Protection: The information system implements **[Assignment: organization-defined cryptographic uses and type of cryptography required for each use]** in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. References: None.	Low, Moderate, High PII Confidentiality Impact Level Parameter Values: … … either FIPS-validated or NSA-approved cryptography to ensure the confidentiality and integrity of PII in transit or at rest… Source: CNSSI 1253 Privacy Overlay
SC-28; SYSTEM AND COMMUNICATIONS PROTECTION; Protection Of Information At Rest: The information system protects the **[Selection (one or more):** **- confidentiality;** **- integrity** **]** of **[Assignment: organization-defined information at rest].** References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … confidentiality and integrity… … PII… Source: CNSSI 1253 Privacy Overlay
SI-7; SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring RENAMED: Software, Firmware, And Information Integrity: The organization employs integrity verification tools to detect unauthorized changes to **[Assignment: organization-defined software, firmware, and information].** References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … PII… PHI Parameter Values: … PHI… Source: CNSSI 1253 Privacy Overlay
SI-10; SYSTEM AND INFORMATION INTEGRITY; Information Input Validation: The information system checks the validity of **[Assignment: organization-defined information inputs].** References: None.	Moderate and High PII Confidentiality Impact Level Parameter Values: … PII… Source: CNSSI 1253 Privacy Overlay

SI-11; SYSTEM AND INFORMATION INTEGRITY; Error Handling: The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to **[Assignment: organization-defined personnel or roles]**. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: b. …authorized individuals with a need for the information in the performance of their duties… PHI Parameter Values: b. … authorized individuals with a need for the information in the performance of their duties… Source: CNSSI 1253 Privacy Overlay

Table 14 - PII/PHI Parameter Values for C/CE Not Included In FedRAMP M or FedRAMP+

AC-3 (9); ACCESS CONTROL; Access Enforcement - Enhancement: Controlled Release The information system does not release information outside of the established system boundary unless: (a) The receiving **[Assignment: organization-defined information system or system component]** provides **[Assignment: organization-defined security safeguards]**; and (b) **[Assignment: organization-defined security safeguards]** are used to validate the appropriateness of the information designated for release. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Value: (a) … organization or information system… … privacy and security controls commensurate with the PII confidentiality impact level of the PII being received… (b) … Appendix J, Controls UL-1 and UL-2… Source: CNSSI 1253 Privacy Overlay
AC-3 (10); ACCESS CONTROL; Access Enforcement - Enhancement: Audited Override Of Access Control Mechanisms The organization employs an audited override of automated access control mechanisms under **[Assignment: organization-defined conditions]**. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … situations where access control mechanisms are overridden for information systems containing PII under the Privacy Act… Source: CNSSI 1253 Privacy Overlay
AC-4 (8); ACCESS CONTROL; Information Flow Enforcement - Enhancement: Security Policy Filters The information system enforces information flow control using **[Assignment: organization-defined security policy filters]** as a basis for flow control decisions for **[Assignment: organization-defined information flows]**. References: None.	High PII Confidentiality Impact Level Parameter Value: …… best available security policy filters, or like technology to filter on selected PII values …… prevention of unauthorized transfer of PII across information system boundaries or domains. Source: CNSSI 1253 Privacy Overlay
AC-4 (17); ACCESS CONTROL; Information Flow Enforcement - Enhancement: Domain Authentication The information system uniquely identifies and authenticates source and destination points by **[Selection (one or more):** **- organization,** **- system,** **- application,** **- individual** **]** for information transfer. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Value: … the applicable organization, system, application, or individual… Source: CNSSI 1253 Privacy Overlay

AC-16; ACCESS CONTROL; Security Attributes: The organization: a. Provides the means to associate **[Assignment: organization-defined types of security attributes]** having **[Assignment: organization-defined security attribute values]** with information in storage, in process, and/or in transmission; b. Ensures that the security attribute associations are made and retained with the information; c. Establishes the permitted **[Assignment: organization-defined security attributes]** for **[Assignment: organization-defined information systems]**; and d. Determines the permitted **[Assignment: organization-defined values or ranges]** for each of the established security attributes. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: a. … a security attribute to demonstrate the user (subject) has completed privacy training in the last year… … for data structures that are known or plan to contain PII, a security attribute of "Contains PII" [having] value of "yes" or "no"… PHI Parameter Value: a. … for data structures that are known or plan to contain PHI, a security attribute of "Contains PHI" [having] value of "yes" or "no"… Source: CNSSI 1253 Privacy Overlay
AC-16 (3); ACCESS CONTROL; Security Attributes - Enhancement: Maintenance Of Attribute Associations By Information System The information system maintains the association and integrity of **[Assignment: organization-defined security attributes]** to **[Assignment: organization-defined subjects and objects].** References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … the user attribute of "Annual PII Training" [to] individuals with access to PII…… … the information attribute of "Contains PII" [to] applicable information… PHI Parameter Value: … the information attribute of "Contains PHI" [to] applicable information…… Source: CNSSI 1253 Privacy Overlay
AC-20 (3); ACCESS CONTROL; Use Of External Information Systems - Enhancement: Non-Organizationally Owned Systems / Components / Devices The organization **[Selection:** **- restricts;** **- prohibits** **]** the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … restricts for PII… Source: CNSSI 1253 Privacy Overlay
AU-12 (3); AUDIT AND ACCOUNTABILITY; Audit Generation - Enhancement: Changes By Authorized Individuals The information system provides the capability for **[Assignment: organization-defined individuals or roles]** to change the auditing to be performed on **[Assignment: organization-defined information system components]** based on **[Assignment: organization-defined selectable event criteria]** within **[Assignment: organization-defined time thresholds]**. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Value: … limited subset of authorized system administrators… … any information system that contains PII … … change in risk based on law enforcement, intelligence, or other credible sources of information or a security incident… PHI Parameter Value: … limited subset of authorized system administrators… … any information system that contains PHI… … change in risk based on law enforcement, intelligence, or other credible sources of information or a security incident… Source: CNSSI 1253 Privacy Overlay

MP-8 (3); MEDIA PROTECTION; Media Downgrading - Enhancement: Controlled Unclassified Information The organization downgrades information system media containing **[Assignment: organization-defined Controlled Unclassified Information (CUI)]** prior to public release in accordance with applicable federal and organizational standards and policies. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Values: … PII… PHI Parameter Values: … PHI… Source: CNSSI 1253 Privacy Overlay
AR-4 ; PRIVACY; Accountability, Audit, And Risk Management - Privacy Monitoring And Auditing : The organization monitors and audits privacy controls and internal privacy policy **[Assignment: organization-defined frequency]** to ensure effective implementation. References: The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06-16, 07-16; OMB Circular A-130.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … concurrent with the organization's security control review schedule…… Source: CNSSI 1253 Privacy Overlay
DI-1 (2); PRIVACY; Data Quality And Integrity - Data Quality - Enhancement: Re-Validate PII The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate **[Assignment: organization-defined frequency]**. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Values: … as frequently as is necessary to ensure the PII is accurate, relevant, timely, and complete; commensurate with the impact of the determination to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office… Source: CNSSI 1253 Privacy Overlay
DM-2 ; PRIVACY; Data Minimization And Retention - Data Retention And Disposal : The organization: a. Retains each collection of personally identifiable information (PII) for **[Assignment: organization-defined time period]** to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses **[Assignment: organization-defined techniques or methods]** to ensure secure deletion or destruction of PII (including originals, copies, and archived records). References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: a. … the time period specified by the National Archives and Records Association (NARA)-approved Records Schedule and the Privacy Act SORN… c. … NSA-approved or FIPS-validated techniques or methods… PHI Parameter Values: Privacy Overlay 108 Attachment 6 to Appendix F 04/20/2015 a. … a minimum of 6 years from the date of its creation or the date when it was last in effect, whichever is later… Source: CNSSI 1253 Privacy Overlay
SA-21; SYSTEM AND SERVICES ACQUISITION; Developer Screening: The organization requires that the developer of **[Assignment: organization-defined information system, system component, or information system service]**: a. Have appropriate access authorizations as determined by assigned **[Assignment: organization-defined official government duties]**; and b. Satisfy **[Assignment: organization-defined additional personnel screening criteria]**. References: None.	Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … systems containing PII…… a. … contracting officer and contracting officer representative, in consultation with the organization's privacy office…… b. … … organization defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII… Source: CNSSI 1253 Privacy Overlay

SC-8 (2); SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity - Enhancement: Pre / Post Transmission Handling The information system maintains the **[Selection (one or more):** **- confidentiality;** **- integrity** **]** of information during preparation for transmission and during reception. References: None.	Moderate and High PII Confidentiality Impact Level Parameter Values: … confidentiality and integrity… Source: CNSSI 1253 Privacy Overlay

This page is intentionally blank.

Appendix F FUTURE Privacy Overlay Guidance

This is a placeholder for a table of Privacy Overlay C/CE along with their applicability and supplemental guidance.

This page is intentionally blank

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu