DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

Version 1, Release 4

14 January 2022

Developed by DISA for the DoD

Trademark Information

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

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

The Cloud Computing (CC) Security Requirements Guide (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 applies to DoD-provided cloud services and those provided by a contractor on behalf of the department, i.e., a commercial cloud service provider or integrator.

Cloud computing technology and services provide the DoD with the opportunity to deploy an enterprise cloud environment aligned with federal government-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 on well-executed security requirements, defined and understood by both DoD components and industry. Consistent implementation and operation of these requirements ensures mission execution, provides sensitive data protection, increases mission effectiveness, and ultimately results in the outcomes and operational efficiencies the DoD seeks.

The Dec. 15, 2014 DoD chief information officer memo *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 CC SRG.

1.1 Purpose and Audience

The CC SRG serves several purposes:

- Provides security requirements and guidance to DoD and commercial cloud service providers (CSPs) that want to have their cloud service offerings 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 provisional authorization (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.

[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)

- Provides guidance to DoD mission owners, Security Control Assessors (SCA), AOs, and others in planning and authorizing the use of a CSO.
- Supports the DoD CIO's Cloud initiative to migrate DoD websites 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 AOs

1.2 Authority

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

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.

DoD Instruction (DoDI) 8500.01, *Cybersecurity*, directs the DISA director, under the authority, direction, and control of the DoD CIO, to develop and maintain Control Correlation Identifiers (CCIs), 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.

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 information classified as 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" that 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 third-party CSO, CSP, or facilities provider (i.e., subcontractor) 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 its Software as a Service (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 that uses or resells one or more CSPs/CSOs to fulfill contract requirements, the CC SRG is applicable to all cloud services.

Note: While *DoDI 8510.01, DoD RMF* requires that IT services and IT products are to be assessed but not authorized, the risks of using cloud computing require a different approach. Therefore, the DoD CIO has determined that a two-step authorization process is required. The first step is to assess the CSP's CSO to determine if it is secure enough to host DoD information and then preliminarily authorize or pre-approve the CSO through the development of a DoD provisional authorization. This process is primarily for commercial CSOs. The second step is for the mission owner's (i.e., the DoD customer of the CSO AO) to be aware of the risk to their specific information by the specific cloud use case and to accept that risk through an ATO.

While the CSP's overall service offering may be inheriting controls and compliance from a third party, the prime CSP, i.e., the CSP or integrator 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*. 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 use similar baselines of the NIST SP 800-53 security controls as the foundation 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 a non-DoD 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.

Notes:

- PaaS CSOs can be services that closely resemble either IaaS or SaaS. This will be better addressed in a future release of this CC SRG.

- While this CC SRG applies to all DoD use cases of cloud computing, one of its primary focus points is facilitating the migration of DoD systems and applications hosted on physical infrastructure 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. It does not address all DoD systems and applications unless they are migrating to or leveraging cloud services. Neither does it address systems and applications used by DoD that are already approved for direct access via the internet 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 SRGs/STIGs

SRGs are collections of security requirements applicable to a given technology family, product category, or 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, STIGs are the detailed guidelines for specific products. 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 each 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) or .xml files, in Extensible Configuration Checklist Description Format (XCCDF) containing the security requirements. Security requirements are presented in the form of 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 using STIGs/SRGs or a configuration guide deemed equivalent by DoD.

1.5 SRG and STIG Distribution

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

Note: Some content requires a DoD Public Key Infrastructure (PKI) certificate for access. The Cyber Exchange website 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

The 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, along with reorganized content, corrected errors, and/or additional clarity. The release schedule can be found at https://cyber.mil/stigs/release-schedule/ or https://public.cyber.mil/stigs/release-schedule/.

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.

The DISA RME, 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 CC, which includes 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, *Cyberspace 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.

2. BACKGROUND

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

This CC SRG introduces terminology and concepts that are unique to cloud computing and DoD's usage of the technology. While this section lists some of the key terms, please refer to Appendix B: Glossary for complete definitions.

2.1 Key Terminology

The following is a list of key terminology which is used throughout this document:

- Cloud Service Provider (CSP)
- Commercial CSP
- DoD CSP
- Non-DoD CSP
- Cloud Service Offering (CSO)
- DoD Cloud Service Catalog[2]
- DoD component
- Mission owner (MO)
- DoD Private CSO
- C/CE (Control/Control Enhancement)
- DoD off-premises
- DoD on-premises
- DoD virtually on-premises

2.2 Cloud Computing, Cloud Service, and Cloud Deployment Models

NIST SP 800-145[3] 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.

[2] 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)

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

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 SaaS, PaaS, and 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 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 attributes "private" and "community" under the "DoD private/community cloud," which refers to a cloud service that is built for the exclusive use of DoD users or tenants. The "Federal government community cloud" 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 used 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 as a subset of IaaS. Any other service models proposed by the vendor (such as Data as a Service) will have to be aligned to one of 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.

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

A 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). CSPs offering SaaS may leverage one or more third-party CSOs (i.e., for IaaS or PaaS) to build out a capability or offering.

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

2.4 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)."

2.5 Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP[4] 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 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[5] requires federal departments and agencies to use 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 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 assessment organization (3PAO).

Note: The American Association for Laboratory Accreditation[6] (A2LA) accredits FedRAMP 3PAOs, with the FedRAMP Program Management Office (PMO) providing final approval.

2.6 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 ensure 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.

2.7 DoD Provisional Authorization

A DoD provisional authorization (PA) is an acknowledgement 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. DoD PAs are granted at

[4] FedRAMP: https://www.fedramp.gov/

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

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

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.

Because 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 cloud service offering leverages another CSP's service offering (e.g., CSP A instantiates its SaaS offering in CSP B's IaaS offering), the DoD PA for CSP A's service offering includes inherited compliance of CSP B. Alternately, CSP A offering an SaaS leverages CSP B, CSP C, and CSP D to provide various functionality for its service offering, then CSP A inherits CSP B's, C's, and D's security posture (compliance or non-compliance). In both cases, CSP A will be contractually responsible for CSP B and must have accountability for controls in its sub-contracts. It is therefore highly recommended that CSPs offering service to DoD only use other CSOs that have a DoD PA. If 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.

NOTICE: While vendors/developers/integrators/CSPs that offer an SaaS CSO instantiated on a third-party I/PaaS CSO that has a FedRAMP P-ATO and a DoD PA (e.g., Amazon Web Services [AWS], Microsoft Azure, etc.) inherit C/CE compliance from that CSO, the SaaS must still be assessed and approved for its own DoD PA (usually this includes a FedRAMP P-ATO) if it is to be used by the DoD. This is because the application itself must be assessed/approved since it must meet many of the same C/CE requirements that the underlying CSO must meet.

Note: DoD PAs are not granted to physical facilities (e.g., a data center) that support cloud infrastructure even if the facility might be considered a CSO if it supports multiple CSPs or multiple tenants' equipment. These are assessed for the physical and environmental controls as part of the CSP's cloud service offering 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 CSP's cloud service offering with a DoD PA that leverages another CSP's service offering with a DoD PA may lose its PA if the leveraged CSO loses its PA. CSPs acting as prime contractor must maintain the PA for their CSO and require all subcontracted 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 loses 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,[7] the DISA AO is responsible for approving and revoking DoD PAs.

CSOs possessing a DoD PA are listed in the DoD Cloud Service Catalog[8]. DoD Component services may also implement approved CSP/CSO listings for their agency's use.

[7]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

[8] 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)

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 and then identify the cloud information impact level that most closely aligns with the defined categorization and information sensitivity. This process leverages the FedRAMP Moderate or High baselines through reciprocity. The cloud information impact levels are further defined in Section 3.1 *Information Impact Levels*.

According to Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*,[9] 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][10]. 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 defines three levels to designate the impact of a loss of confidentiality or a loss of integrity (refer to Table 3-1). The security control baseline for all impact levels (ILs) is based on moderate confidentiality and moderate integrity (while ignoring availability) (i.e., MMx). 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 may consider leveraging the FedRAMP High Baseline to support DoD high confidentiality and high integrity (i.e., HHx) workloads in the commercial cloud.

[9] FIPS 199: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[10] 44 U.S.C., Sec. 3542: http://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

Table 3-1: 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 address the impact of availability. The mission owner is expected to 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 four weeks in advance and shall not exceed four hours per month," 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.

3.1 Information Impact Levels

DoD has developed information impact levels (ILs) to segregate major types of information into "buckets" depending on the information's audience and sensitivity. This requires different protections and treatments than the basic RMF information categorization of low, moderate, and high as defined by NIST and used by FedRAMP or the rest of the Federal Government. For example, the FedRAMP baselines do not address National Security Systems/information or

classified information, which is under the purview of the Committee on National Security Systems (CNSS).

The DoD information impact levels defined here consider the potential impact should the confidentiality or the integrity of the information be compromised. Availability considerations are not included beyond that already included under FedRAMP. Availability of any given cloud service must be considered by the mission owner's AO based on the availability advertised by the CSP for their CSO.

NOTICE: There is no such construct as FedRAMP IL2, FedRAMP IL4, or FedRAMP IL5. ILs are a DoD construct only. Do not refer to a FedRAMP L, M, or H P-ATO as having any association with a DoD IL. Do not refer to a DoD PA for a given DoD IL as a FedRAMP IL#.

Note: The previously published (and now superseded) cloud security model[11] defined six information ILs. To simplify the selection process, the number of levels was reduced from six to four in the CC SRG. This was accomplished by integrating levels 1 (public information) and 3 (low impact Controlled Unclassified Information [CUI]) into IL2/4, respectively. The numeric designators for the impact levels were not changed to remain consistent with previous versions of the cloud security model, leaving IL2/4/5/6. The intent was to reduce confusion in the community. Note that a higher level can process data from a lower level.

Additionally, the categorization for the information being stored, processed, or transmitted in the cloud for all levels has been changed to moderate confidentiality and moderate integrity as defined by CNSSI 1253. This modification for IL5/6 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.

DoD does not support the use of the FedRAMP High Baseline for the deployment of mission owners' systems and information categorized at high confidentiality or integrity. Mission owners with such information must deploy to CSOs and facilities assessed using CNSSI 1253 high baselines through the DoD RMF (typically in a DoD facility) or contract for the added security from a commercial CSP. DISA may consider how to incorporate the FedRAMP High Baseline into this SRG in support of DoD high confidentiality and high integrity workloads in the commercial cloud. Until such time, this SRG and DoD only support the deployment of Mission owners' systems and information categorized at moderate confidentiality or integrity.

NOTICE: FedRAMP provides low, moderate, and high baselines for CSPs/CSOs.

Figure 3-1: Impact Level Comparison provides a summary of the current information impact levels coupled with some of the distinguishing requirements and characteristics discussed later in this SRG.

Figure 3-1: Impact Level Comparison

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

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	CSP PERSONNEL REQUIREMENTS & INVESTIGATION EQUIVALENCY
2	PUBLIC	FedRAMP Moderate Baseline (MBL)	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	Tier 1 (T1)
4	CUI (FOUO, PII, PHI) or Non-CUI	Level 2 + CUI-Specific Tailored Set OR FedRAMP HBL	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 (IT-1) Tier 5 (T5)
5	CUI (FOUO, PII, PHI), U-NSI/NSS	Level 4 + NSS-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 (IT-2) Tier 3 (T3) Non-Disclosure Agreement (NDA)
6	Classified SECRET NSS	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 T5 & SECRET Clearance NDA

Notes:

- Refer to Section 5.2.1, Jurisdiction/Location Requirements, for the explanation of "US/US outlying areas".
- ADP-1 and ADP-2 Personnel Requirements apply to both ILs 4 and 5. Refer to Sections 5.6.2, 5.6.2.1, 5.6.2.2, and 5.6.2.3.
- IL4/5 off-premises CSO connectivity will be via a BCAP on any DISN network (e.g., DREN) it serves.

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

3.1.1 Impact Level 2: Non-Controlled Unclassified Information

Impact level 2 accommodates publicly releasable data or non-public unclassified data where the unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations and assets, or individuals. This includes all data cleared for public release as well as some low confidentiality unclassified information NOT designated as CUI or military/contingency operations mission data. However, the information may require some minimal level of access control (e.g., user ID and password). This IL accommodates non-CUI information categorizations based on CNSSI-1253 up to low confidentiality and moderate integrity (L-M-x).

Commercial IL2 CSP/CSO customers include whomever the CSP chooses to market the CSO to, which may include government customers, commercial customers, and the general public. Access to the CSO is via the internet.

3.1.2 Impact Level 4: Controlled Unclassified Information

Impact level 4 accommodates non-public, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations and assets, or individuals. This encompasses CUI and/or other mission data, including that used in direct support of military or contingency operations. 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)12, Part 2002 of 32 CFR13, the CUI Registry 14 and DOD Instruction 5200.48. 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 mission data to be protected at IL4 is the responsibility of the owning organization. Determination of the appropriate IL 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 IL4/5 CSOs without additional assessment over and above the DoD PA. (e.g., for Privacy). This IL accommodates CUI information categorizations based on CNSSI-1253 up to moderate confidentiality and moderate integrity (M-M-x).

For more information on CUI categories, see the National Archives CUI registry.[15] IL4 CSOs may support a U.S. Government Community or a DoD-only community (i.e., the CSO is DoD Private).

Commercial IL4 CSP/CSO customers include all U.S. government customers (federal, state, local, and tribal) and commercial customers that support them. In some cases, an IL4 PA may be granted to CSOs that support other commercial entities, but not the general public.

Commercial IL4 CSO customers include the following:

- DISN NIPRNet-based DoD components – DoD components whose primary network connection to other DoD components and the internet is via NIPRNet. Such DoD components' primary internet access is via the DISN NIPRNet internet access points (IAPs).
- DoD contractors operating a system or application for the DoD. This is primarily for the fulfillment of the contract, not for the contractor's general storage/processing of CUI/ covered defense information (CDI) or the contractor's internal corporate cloud use cases.

[12] EO 13556: https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

[13] Part 2002 of 32 CFR: https://www.gpo.gov/fdsys/granule/CFR-1998-title32-vol6/CFR-1998-title32-vol6-part2002

[14] CUI Registry: https://www.archives.gov/cui/registry/category-list.html

[15] CUI Categories: http://www.archives.gov/cui/registry/category-list.html

In this case, the contractor is operating on the behalf of a mission owner and must fulfill all mission owner requirements as specified in the CC SRG.
- NIPRNet connected but separate COI mission partner networks; e.g., MedCOI, DREN.
- Non-NIPRNet-based DoD components; e.g., commissary, .edu organizations.
- Federal, state, local, tribal government agencies.
- DoD contractors required to store/process DoD CUI or covered defense information (CDI) as part of their DoD contract. This is primarily for the fulfillment of the contract, not for the contractor's internal corporate cloud use cases.

Impact level 4 customer CSO connectivity:

- NIPRNet-based DoD components connect via DoD-provided, DoD CIO-approved NIPRNet boundaries and associated private connectivity.
- Non-NIPRNet-based DoD components connect via DoD component-provided, DoD CIO-approved, and Non-NIPRNet boundaries and associated private connectivity. Alternate connectivity methods must be approved by DoD CIO.
- All other CSO customers establish their own boundaries and private or internet-based connectivity.

Refer to Section 5.10.1: Cloud Access Point (CAP) for information on DoD NIPRNet to CSO boundaries.

3.1.3 Impact Level 5: Controlled Unclassified Information and Unclassified National Security Information (U-NSI)

Impact level 5 accommodates non-public, unclassified National Security System (NSS) system data (i.e., U-NSI) or non-public, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. This includes CUI and/or other mission data that may require a higher level of protection than that afforded by IL4 as deemed necessary by the information owner, public law, or other government regulation. The determination of whether CUI and/or mission data fits this category is up to the AO responsible for categorizing the information and choosing the cloud impact level.

IL5 also supports unclassified NSSs due to the inclusion of NSS-specific requirements in the FedRAMP+ C/CEs. Therefore, NSS must be implemented at IL5. Some types of CUI may not be eligible to be hosted on IL4/5 CSOs additional assessment over and above the DoD PA (e.g., for privacy). This IL accommodates NSS and CUI information categorizations based on CNSSI-1253 up to moderate confidentiality and moderate integrity (M-M-x). As noted in 3.2 above, DoD and this SRG do not support information categorized as high confidentiality and high integrity (H-H-x) being deployed in commercial CSOs at this time.

IL5 CSOs may support a federal government community or a DoD-only community (i.e., the CSO is DoD Private). Commercial IL5 CSO customers include the following:

- DISN NIPRNet-based DoD components (i.e., DoD components whose primary network connection to other DoD components and the internet is via the DISN unclassified

network service called NIPRNet). Such DoD components' primary internet access is via the DISN NIPRNet IAPs.
- NIPRNet connected but separate COI mission partner networks; e.g., MedCOI, DREN
- Non-NIPRNet based DoD components; e.g., commissary, .edu organizations
- Federal agencies operating an unclassified NSS
- Federal agency and DoD contractors operating a system or application (to include an unclassified NSS) for the federal agency or DoD. This is primarily for the fulfillment of the contract, not for the contractor's general storage/processing of CUI/CDI or the contractor's internal corporate cloud use cases. In this case, the contractor is operating on the behalf of a mission owner and must fulfill all mission owner requirements as specified in the CC SRG.

Impact level 5 customer CSO connectivity:

- NIPRNet-based DoD components connect via DoD-provided, DoD CIO-approved, NIPRNet boundaries and associated private connectivity.
- Non-NIPRNet-based DoD components connect via DoD component-provided, DoD CIO-approved, non-NIPRNet boundaries and associated private connectivity. Alternate connectivity methods must be approved by DoD CIO.
- All other CSO customers establish their own boundaries and private or internet-based connectivity.

Refer to Section 5.10.1, Cloud Access Point (CAP), for information on DoD NIPRNet to CSO boundaries.

3.1.4 Impact Level 6: Classified Information Up to SECRET

Impact level 6 accommodates non-public, classified NSS system data (i.e., classified national security information [NSI]) or non-public, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals). That is information that has been determined: "(i) pursuant to EO 12958, *Classified National Security Information* (April 17, 1995) as amended by EO 13292[16], 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)[17] 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 IL. Access to the CSO is via one or more private SIPRNet (SECRET Internet Protocol Router Network) connections. IL6 accommodates classified information categorizations up to moderate confidentiality and moderate integrity (M-M-x). Classification does not dictate a high (H-H-x) information categorization. As noted in 3.2 above, DoD and this SRG do not support information categorized as high confidentiality and high integrity (H-H-x) being deployed in commercial CSOs at this time.

[16] EO 12958 as amended by EO 13292: http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html

[17] AEA 1954 as amended: http://pbadupws.nrc.gov/docs/ML1327/ML13274A489.pdf#page=23

IL6 CSOs may support a Federal Government Community or a DoD-only community (i.e., the CSO is DoD Private). Due to the requirement that the entire CSO infrastructure be dedicated and separate from other CSP/CSO infrastructure, IL6 CSOs may only be provided by CSPs under contract to the DoD or a Federal Agency. In this sense, the CSO is not considered "commercial" or "commercially available" even though the CSO infrastructure is expected to be an exact or close copy of the given CSP's commercial offering.

Impact level 6 CSO customers include the following:

- DISN SIPRNet-based DoD components, i.e., DoD components whose primary network connection to other DoD components for Secret classified communications is via the DISN Secret network service called SIPRNet.
- Federal agencies whose networks are part of the "National Secret Fabric" and/or are connected to SIPRNet
- SIPRNet connected but separate COI mission partner Secret networks; federal agency Secret networks.
- DoD contractors operating a Secret NSS for the DoD. This is primarily for the fulfillment of the NSS contract, but might also be used (if approved) for the contractor's general storage/processing of Secret CDI.

4. RISK ASSESSMENT/AUTHORIZATION 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 ILs (discussed in Section 3.1, *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 IL(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 IL 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 AO 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/Validation, Risk Assessment (informed by Security Control Assessment), Ongoing Assessment (continuous monitoring), and System Authorization." While *DoDI 8510.01, DoD RMF* requires that IT services and IT products are to be assessed but not authorized, the risks of using cloud computing require a different approach. As such, the DoD CIO has determined that a two-step authorization process is required when leveraging commercial CSOs. The first step is to assess the CSP's CSO to determine if it is secure enough to host DoD information then preliminarily authorize or pre-approve the CSO through the development of a DoD PA. (Refer to Section *2.6, DoD Provisional Authorization for additional information*) The second step is for the mission owner's (i.e., the DoD customer of the CSO) AO to be aware of the risk to their specific information by the specific commercial cloud use case, and to accept that risk through an ATO.

The following lists the relationship between DoD PA and DoD or mission owner's ATOs and the associated CSOs:

- Commercially owned and commercially operated (COCO) on- or off-premises CSOs will be assessed for a DoD PA. This includes IaaS, PaaS, and SaaS.
  - For IaaS/PaaS, the mission owner must develop an assessment package for the application/system built upon the CSO.
  - For IaaS/PaaS, the mission owner's AO must accept the risk of hosting their information in the CSO based on the PA and the mission owner's assessment package.
  - For SaaS, the mission owner's AO must accept the risk of hosting their information in the CSO through the development of an ATO (unless an enterprise level ATO exists for the CSO) based on the PA.

- COCO on- or off-premises CSOs designated by DoD CIO and DISA as an enterprise service will be assessed for a PA then based on this, awarded an enterprise ATO that can be leveraged by any DoD component through reciprocity.
- Government owned/operated (GOGO) or Government owned contractor operated (or commercially operated) (GOCO) on-premises CSOs will be awarded an ATO.
    - If designated by DoD CIO and DISA as an enterprise service the CSO will be assessed then awarded an enterprise ATO that can be leveraged by any DoD component through reciprocity.

If a DoD Component owns the CSO infrastructure, then the CSO will be assessed and Component AO will award the ATO.

4.1 Assessment of Commercial and Non-DoD Cloud Services for Enterprise Use

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 3.1, Impact level 2 information may be hosted in a CSP that is provisionally authorized as FedRAMP compliant at the moderate or high level through full reciprocity. The two acceptable government authorizations include:

- JAB PA – Based on a determination by the JAB that an acceptable level of risk exists for leveraging across the federal government. DoD/DISA 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 require additional NIST 800-53 RMF control assessments at IL2 any CSP/CSO compliant at the FedRAMP moderate or high level may be used at DoD IL2 without a written DoD PA. In the event such a CSO becomes too risky for DoD use, DISA will rescind their automatic DoD IL2 PA via a written memo.

NOTICE: In the event a DoD component requires a CSO to fulfill mission needs at IL2 that does not have a FedRAMP moderate (or higher) JAB P-ATO or agency ATO, i.e., not on the FedRAMP Marketplace, the DoD component may assess and authorize the CSO then submit their ATO to FedRAMP for inclusion on the marketplace providing the CSO will not be submitted for a IL4/5 DoD PA in the future.

Impact level 4/5: RMF assessments for IL4 and above are based on a combination of the security controls in the FedRAMP moderate or high baselines and the DoD specific controls/requirements outlined in Section 5.1.2*, DoD FedRAMP+ Security Controls/Enhancements* and other requirements 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. Subsequent to the

validation of the Security Assessment Report (SAR), 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 approves DoD PAs for the DoD CIO.

NOTICE: A DoD component must sponsor a CSP/CSO for a DoD IL4/5/6 PA. The component sponsor must provide experienced NIST SP 800-53 C/CE validators to help with the validation of the CSP's CSO SAR. Application for sponsorship is accomplished through the DoD Cloud Authorization Services (DCAS) website[18].

There are three paths that can be followed in assessing a CSP for a IL4/5 DoD PA and subsequent listing in the DoD Cloud Service Catalog[19] 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 IL4 and above. CSPs having a FedRAMP JAB PA have been assessed by an accredited/approved 3PAO against the FedRAMP moderate or high 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 DISA SCA and the DoD CIO have already been involved in the FedRAMP validation 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 acceptable minimum baseline is FedRAMP moderate. The information from the non-DoD agency ATO will be supplemented with an assessment of the DoD-specific controls and requirements not addressed by FedRAMP for ILs4 and above. This additional assessment should be performed by the CSP's 3PAO and submitted to the DISA SCA for review and validation 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.

[18] DCAS Website: https://disa.deps.mil/org/RMED/cas/SitePages/CASHome.aspx

[19] 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)

NOTICE: This path is not available to CSP's CSOs having a DoD component ATO; as such a CSO may only be used at DoD IL2. DoD agency ATOs must be signed and submitted to FedRAMP by the DISA AO for the DoD CIO.

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

  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.

  In this case, the CSP's CSO is fully assessed, independent of the FedRAMP PMO, by a FedRAMP accredited/approved 3PAO in coordination with the DISA cloud SCA organization. The CSP's CSO must be assessed against both the FedRAMP moderate (or high) baseline and FedRAMP+ requirements.

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

  If a CSP receives a DoD assessed PA, and that service offering may be leveraged by other federal agencies, the CSP's assessment package may be shared with, and be available through, the FedRAMP Marketplace as well as the DoD Cloud Services Catalog. In this case, the DoD PA signed by the DISA AO serves as a DoD agency ATO for FedRAMP reciprocity. 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 O&O Cloud Services and Enterprise Services Applications.*

NOTICE: DoD PAs must be signed by the DISA AO for the CSO to be used by multiple DoD components (the enterprise) or to serve as a DoD agency ATO for submission to FedRAMP for use by other federal agencies. ATOs for a CSO signed by a DoD component AO only permit the CSO to be used within that DoD component.

CSOs may (should) 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-U.S. 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.*

Impact level 6 off-premises: Assessment and authorization of off-premises DoD contractor facilities and information systems that process, store and transmit classified information (i.e., non-DoD commercial CSPs and their IL6 CSOs) must be performed in conjunction with the National Industrial Security Program (NISP) (as defined in Executive Order 12829[20]) and the Industrial Security Regulation (ISR) (DoD 5220.22-R)[21] in accordance with 48 Code of Federal Regulations (CFR) Subpart 4.4 - Safeguarding Classified Information within Industry[22] and Federal Acquisition Regulations (FAR) Section 52.204-2 - Security Requirements[23]. 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[24] 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 IL6 offerings must adhere to the National Industrial Security

[20] EO 12829, NISP: http://www.archives.gov/isoo/policy-documents/eo-12829.html

[21] DoD 5220.22-R: http://www.dtic.mil/whs/directives/corres/pdf/522022r.pdf

[22] 48 CFR Subpart 4.4:

https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4-subpart4-4

[23] FAR 52.204-2:

https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf

[24] DoDI 5220.22 NISP: http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf

Program Operating Manual (DoD 5220.22-M) [25]. Together the ISR, NISPOM, and Office of the Designated Approving Authority (ODAA) Process Manual[26] provide guidance.

Notes:

- It is the intent of the DoD CIO that all CSPs and CSOs are assessed against the same set of requirements and cybersecurity 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 IL6 will be coordinated with OUSD(I) and DSS as NISP policies and procedures are updated. Notwithstanding the above, IL6 CSOs must be assessed using the FedRAMP moderate or high baseline, the IL6 FedRAMP+ C/CE and the CNSSI 1253 Appendix F, Attachment 5 *Classified Information Overlay* C/CEs following FedRAMP processes using a 3PAO to receive a DoD PA. DISA and DSS will jointly validate the SAR. Refer to Section *5.1.4.1, NSS Level 6 Classified Overlay Applicability* for additional information.

- While NISP policies dictate that DSS will accredit all IT in a contractor facility, providing full application ATOs, this is not appropriate or efficient for IL6 cloud use cases. IL6 processes should mirror the processes for IL4/5 except for facility and personnel clearances. As such, DSS authorizes the facility clearances required and coordinates with DISA for the DoD PA. The mission owner is still responsible for producing their ATO for using and placing their classified information in the IL6 CSO as they are with all other unclassified levels.

- Many feel that the existence of classified information requires that it and/or the system be categorized as high and protected accordingly by assessing systems using the FedRAMP high baseline or a CNSSI 1253 HHH baseline. This is not true. In accordance with (IAW) the *Classified Information Overlay* which states "the categorization decision (i.e., the impact values for confidentiality, integrity, and availability) is independent of the classification decision," there is no requirement that drives classified information/systems to be categorized as high; thus, no requirement to assess/authorize them using a high baseline.

Impact level 6 on-premises: Assessment and authorization of on-premises IL6 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

[25] DoD 5220.22-M, NISPOM: http://www.dss.mil/documents/odaa/nispom2006-5220.pdf

[26] (ODAA) Process Manual: http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf

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 IL6 CSOs will be minimally assessed IAW the FedRAMP moderate or high baseline, the IL6 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. Refer to Section *5.1.4.1, NSS Level 6 Classified Overlay Applicability* for additional information.

Note: Refer to Section 5.6.2.2, *CSP Personnel Requirements – PS-3: Background Investigations* under the IL6 topic for additional requirements related to on-premises contractor- managed CSOs WRT organizational facilities clearances and cleared personnel.

4.1.1 Assessment of On-Premises Commercially Owned and Operated Cloud Services

On-premises commercially owned and operated (COCO) cloud services (e.g., milCloud2 IaaS/PaaS or other SaaS) intended as a DoD-wide enterprise service are subject to the same requirements found in this SRG and the same security controls as commercial CSOs. As such, a DoD PA is required before going into production.

Similarly, on-remises COCO cloud services instantiated by DoD components may assess and authorize the CSO under a component ATO using the same requirements found in this SRG and the same security controls as commercial CSOs. The component ATO will only permit the CSO to be used by that component. ATOs will not be considered for a DoD PA.

4.1.2 DoD Component Sponsorship of a CSO for a FedRAMP Agency ATO

DoD components are not permitted to submit DoD PAs or component ATOs as a DoD agency ATO for inclusion on the FedRAMP Marketplace. The DoD CIO represents DoD as the agency in this capacity, thus only DoD assessed PAs/ATOs signed by the DISA AO (representing the DoD CIO) may be submitted to FedRAMP as an agency ATO.

4.2 Assessment of DoD O&O Cloud Services and Enterprise Services Applications

DoD owned and operated (O&O) and government owned and commercially operated (GOCO) CSOs (e.g., original milCloud IaaS/PaaS) are subject to the same requirements found in this SRG and the same security controls as commercial CSOs. However, DoD CSP/CSO 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. This means the DoD CSO must be assessed against the aggregate baseline made up of the appropriate FedRAMP baseline (minimally moderate) and the appropriate CNSSI 1253 baselines (as tailored) for the CSO. DoD O&O CSOs require a full ATO which may be used in lieu of a PA or to generate a PA that can be leveraged by mission owners and their AOs.

DoD enterprise service programs that might be considered cloud services under the SaaS model [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 baselines. Such programs are DoD-assessed as noted above, not subject to being assessed through the FedRAMP program, and do not share DoD ATOs with the FedRAMP secure repository.

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 is provided and addressed with the CSO versus what is 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 4 1: 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 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 IL. At IL4 and above, it is 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 available for use across the DoD by multiple 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 ILs. This mission

system ATO requirement extends to DoD CSP IaaS/PaaS CSOs, where an ATO has been granted instead of a PA, since its ATO or PA only permits its connection to the DISN and such an ATO cannot address full mission system/application risk when built on the CSO. While a mission owner may use a DoD CSP SaaS, CSOs having an ATO without creating a separate ATO, the ATO requirement still applies to a DoD CSP SaaS CSOs only having a PA.

Note: While *DoDI 8510.01, DoD RMF* requires that IT services and IT products are to be assessed but not authorized, the risks of using cloud computing require a different approach. As such, the DoD CIO has determined that a two-step authorization process is required. The first step is to assess the CSP's CSO to determine if it is secure enough to host DoD information then preliminarily authorize or pre-approve the CSO through the development of a DoD PA. This process is primarily for commercial CSOs. The second step is for the mission owner's (i.e., the DoD customer of the CSO) AO to be aware of the risk to their specific information by the specific cloud use case, and to accept that risk through an ATO.

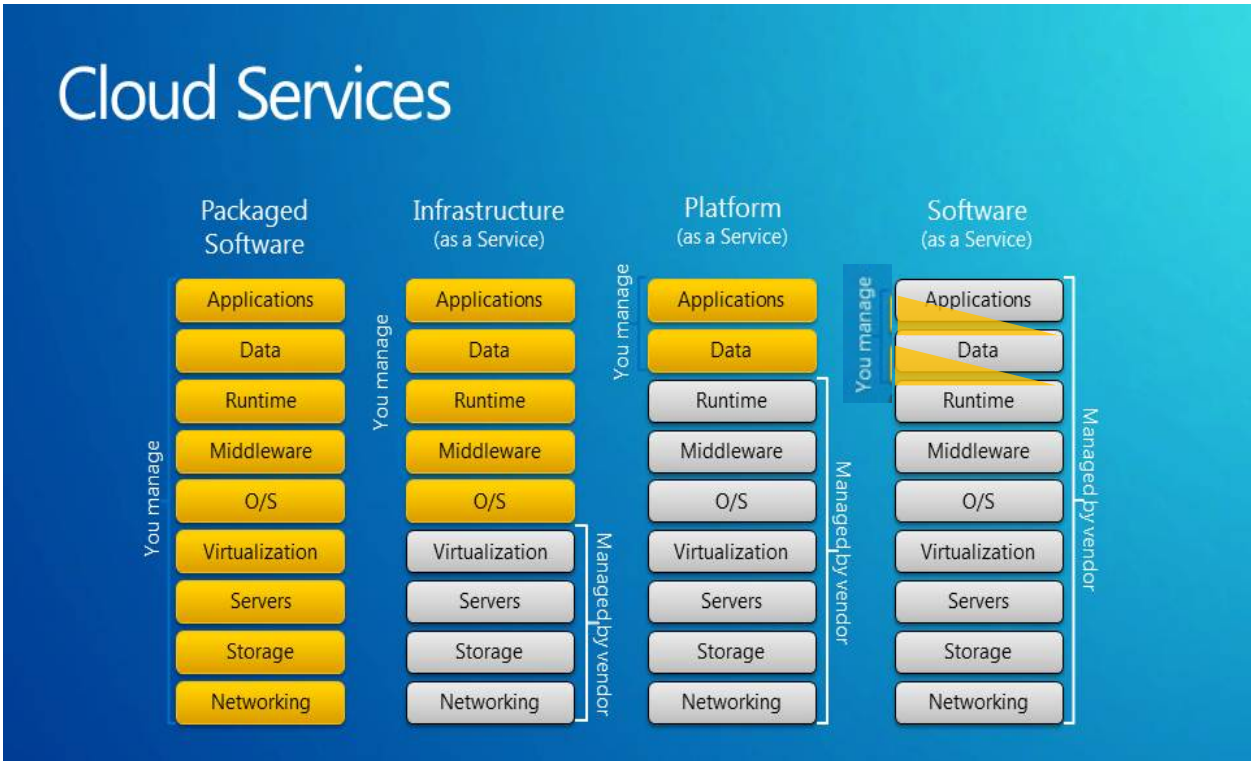
The requirement that a mission owner must only use CSOs that have a DoD PA extends to CSOs provided by a third-party integration contractor or reseller of CSP CSOs. Any CSO being integrated into a solution for use by DoD or resold to a DoD entity must have a DoD PA.

Mission owners categorize mission systems and/or applications 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 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 ILs and additional overlay controls (e.g., privacy). While Figure 4-1 depicts the division of management and ergo responsibility shared between the CSP and mission owner, it also illustrates the concept of inheritance.

Figure 4-1: Notional Division of Security Inheritance and Risk[27]

[27] Figure 2: Graphic courtesy of Microsoft



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.

4.4 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 MBL or HBL 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 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; DFARS Interpretation

This section provides information relative to PAs and ATOs in relation to 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, but is intended to provide additional clarity primarily regarding on-premises CSOs.

This topic must be addressed from two viewpoints. These are:

1- When the commercial CSO infrastructure is off-premises (where it is typically already in existence), vs
2- When the CSO infrastructure is contracted to be on-premises either physically or virtually (where it typically will need to be built using dedicated hardware).

Off-premises commercial service: IAW DFARS SUBPART 239.76—CLOUD COMPUTING,[28] 239.7602-1 (b)(1), a CSP must have a DoD PA at the appropriate information impact level (IIL) before contract award. In essence, this means the CSP/CSO must typically have a DoD PA before responding to a DoD cloud services RFP or show evidence that the CSO can achieve a DoD PA before contract award. This may not be practical for meeting contract requirements and customer needs in a timely manner.

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 at the appropriate IIL.

DFARS 239.7602-1 (b)(2) provides 2 exceptions:

1. The requirement is waived by the DoD CIO.

2. "The cloud computing service requirement is for a private, **on-premises** version that will be provided from U.S. government facilities. Under this circumstance, the cloud service provider must obtain a provisional authorization prior to operational use." This is clarified below.

[28] DFARS **SUBPART 239.76: http://www.acq.osd.mil/dpap/dars/dfars/html/current/239_76.htm#239.76**

Additionally, in the case of a mission owner leveraging a commercial off-premises CSO and its PA, the mission owner's AO provides the ATO for their usage of the CSO to meet DoD RMF policy. This is also covered in the DoD CIO's cloud memo.

On-premises (physically or virtually): While the general DFARS rule applies to on-premises CSOs in that it is beneficial to DoD that the commercial instantiation of the CSP's CSO has been assessed and awarded a DoD PA, proving the commercial service and infrastructure is capable of hosting DoD information and systems at the appropriate IIL, this PA is not directly useable for a separate on-premises instantiation of the CSO.

An on-premises CSO is DoD private which will be connected to a DISN service (i.e., NIPRNet or SIPRNet) as described elsewhere in the CC SRG. As such, the CSO must have a DoD interim authority to test (IATT), conditional ATO, or PA to connect to the network for testing and a DoD ATO with or without conditions before going into production IAW normal DoD policy. A previous DoD PA for the off-premises commercial instantiation will only inform the assessments for the on-premises IATT and ATO. Certain portions of the previous PA assessment will have to be re-assessed due to the new infrastructure and different location(s), while some C/CE compliance will be inherited from the DoD and specific facility where the CSO infrastructure is located rather than the commercial facility. In a virtually on-premises scenario, the instantiation might inherit some C/CE compliance from the DoD PA for the commercial service and the commercial datacenters where it is hosted, providing the private instantiation is hosted in the same datacenter(s) as were reviewed for the PA. Refer to Section 5.2.1.1, *DoD Off-Premises Vs On-Premises Vs Virtually On-Premises* for additional information.

As noted above, DFARS clause 239.7602-1.(b)(2)(ii), provides for an exception to the general rule that a CSP/CSO must have a DoD PA before award. It states that a contract may be awarded for a private on-premises CSO that will be provided from U.S. government facilities. It further states that the CSO must obtain a PA prior to operational use. Alternately, on-premises DoD systems to include CSOs may require an ATO before operational use. This ATO may be used in lieu of a PA or to generate a PA to be leveraged by mission owner's and their AOs.

NOTICE: While an RFP may require that a CSO must meet all of the requirements outlined in the DoD CC SRG for IL2/4/5/6, this excludes on-premises CSOs regarding a PA before award. Furthermore, unless a CSP already offers an IL6 CSO that has a IL6 PA, it is impossible obtain a DoD IL6 PA before a contract award, because an IL6 PA cannot be obtained by a CSP unless a contract is in place that generates a DD-254, thus allowing a DSS facility clearance to be obtained for the facilities housing the CSO. Unless a CSP has other contracts whereby their CSO is already in a facility with a facility clearance, an IL6 PA cannot be granted.

4.6 Cloud Service vs. a Managed IT Service

In accordance with industry norms, a managed IT service is one where the customer dictates the technology and the operational procedures while for a cloud service the provider (i.e., CSP) dictates the technology and the operational procedures. A physically or virtually on-premises DoD private CSO operated by a contractor, whether that contractor is the original CSP or other organization, can be a managed service rather than a cloud service in the usual sense. This can happen when DoD contracts for a "copy" or "version" of a CSP's commercial cloud service to be built on DoD premises (virtually or physically) and operated/managed as a private CSO.

Whether it is a managed service vs cloud service depends on how many of the requirements for the service, its infrastructure, and management DoD specifies or dictates.

DoD private managed services are subject to normal DoD security requirements and RMF policy rather than DoD policy addressing commercial cloud services. The applicable security requirements for a managed cloud service will include requirements in this CC SRG and standard DoD RMF security requirements.

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 and DoDI 8510.01 require 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.

> **DoDI 8500.01**, March 14, 2014 2.g(1) (1) All DoD IS and PIT systems will be categorized in accordance with Reference (ci) and will implement a corresponding set of security controls that are published in Reference (cj) regardless of whether they are National Security System (NSS) or non-NSS.
>
> (ci) Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 15, 2012, as amended
>
> (cj) National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," current edition
>
> **DoDI 8510.01**, March 12, 2014 3. d. All DoD IS and PIT systems must be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253 (Reference (e)), implement a corresponding set of security controls from NIST SP 800-53 (Reference (f)), and use assessment procedures from NIST SP 800-53A (Reference (g)) and DoD-specific assignment values, overlays, implementation guidance, and assessment procedures found on the Knowledge Service (KS). As supporting reference security control documents are updated, DoD's implementation of these updates will be coordinated through the RMF TAG.
>
> **Note:** "implement a corresponding set of security controls" means as defined by the corresponding 1253 aggregate baseline.

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.

Refer to NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*,[29] for a definition of NSS and further information.

5.1.1 DoD Use of FedRAMP Security Controls

The FedRAMP low, moderate and high baselines are a tailored set of C/CEs based on the low, moderate and high 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 moderate baseline at all information ILs and considers the high Baseline at some.

Impact level 2: 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, IL2 information may be hosted in a CSP that minimally holds a FedRAMP moderate or high PA; subject to compliance with the personnel security requirements outlined in Section 5.6.2, *CSP Personnel Requirements* and acceptance by the mission owner and the responsible AO. Only FedRAMP moderate or high baseline controls will be assessed for DoD PAs for IL2. DoD provides full reciprocity with FedRAMP moderate and high P-ATOs for DoD IL2. This in no way alleviates the CSP from meeting other security and integration requirements for CSP's/CSOs as required by the mission owner while hosting DoD IT missions or the mission owner from securing their systems/websites/applications in IL2 CSOs.

Impact level 4: The FedRAMP moderate baseline, supplemented with DoD FedRAMP+ C/CEs and other requirements in this SRG, are used to assess CSPs toward awarding a DoD PA at information IL4.

An alternate path to a DoD IL4 PA is available due to coordination of the FedRAMP high baseline and DoD IL4 FedRAMP+ C/CE. A FedRAMP high PA will be accepted for a DoD Level 4 PA without additional C/CE assessment, however, assessment of non-C/CE based requirements in this SRG is required.

Impact levels 5/6: The FedRAMP moderate or high baseline, supplemented with DoD FedRAMP+ C/CEs and requirements in this SRG, are used to assess CSPs toward awarding a DoD PA at information IL56.

No matter what C/CE baseline is used as the basis for a FedRAMP PA, additional considerations and/or requirements will need to be assessed and approved before a DoD PA can be awarded at IL4/5/6. These considerations and/or requirements can be found throughout this SRG, while a summary can be found in Section 5.1.7, Additional Considerations and/or Requirements for IL4/5 DoD PA Award.

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

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 IL, except for IL2. These baselines incorporate, but are not limited to, the FedRAMP moderate or high baselines. 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 IL. This comparison indicated that the FedRAMP moderate baseline includes approximately 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 IL.

More recently, with the development of the FedRAMP high baseline, a portion of the DoD IL4 FedRAMP+ C/CE was accepted for inclusion into the FedRAMP high baseline along with several value adjustments.

Table 5-1 provides a listing of the FedRAMP+ C/CEs applicable to each information IL, which includes only three additional base controls. 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 or high baseline C/CEs, tables of which can be obtained from the FedRAMP website on the documents page[30].

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

Table 5-1: DoD FedRAMP+ Security Controls/Enhancements

SP 800-53r4 Cont./Enh. ID	FedRAMP+ for FedRAMP Moderate Baseline			FedRAMP+ for FedRAMP High Baseline		
	IL 4	IL 5	IL 6	IL 4	IL 5	IL 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*		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			

SP 800-53r4 Cont./Enh. ID	FedRAMP+ for FedRAMP Moderate Baseline			FedRAMP+ for FedRAMP High Baseline		
	IL 4	IL 5	IL 6	IL 4	IL 5	IL 6
PL-08 (01)		X	X		X	X
PS-04 (01)		X	X		X	X
PS-06 (03)		X	X		X	X
SA-04 (07)		X	X		X	X
SA-12	X	X	X			
SA-19	X	X	X			
SC-07 (10)	X	X	X			
SC-07 (11)		X	X		X	X
SC-07 (14)			X			X
SC-08 (02)		X	X		X	X
SC-23 (01)	X	X	X			
SC-23 (03)	X	X	X			
SC-23 (05)		X	X		X	X
SI-02 (06)	X	X	X			
SI-03 (10)		X	X		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		X	X
SI-10 (03)	X	X	X			
Total	Also refer to 5.1.5	Also refer to 5.1.4 5.1.5	Also refer to 5.1.4 5.1.4.1			
*** Most IL 5 FedRAMP+ C/CEs are also applicable at IL 6. The use of n/a in IL 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 3PAO assessed 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 ILs are based on those from CNSSI 1253, only impact ILs5/6 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, all 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*.[31] 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 Personally Identifiable Information (PII)/Protected Health Information (PHI) in the Cloud

Personally Identifiable Information (PII) and Protected Health Information (PHI) are categorized as CUI and, as such, PHI and most PII in the cloud must minimally be protected in a Level 4 CSO. Most PII refers to PII categorized as having a moderate or high (and some low not meeting the exception below) confidentiality impact level as determined in accordance with *NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*[32].

Mission owner PII impact level determinations will be performed as part of the information system's privacy impact assessment per DoD Instruction 5400.16, "*DoD Privacy Impact Assessment (PIA) Guidance*",[33] and documented in Section 2.b. of DD Form 2930 "*Privacy*

[31] Classified Information Overlay: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[32] NIST SP 800-122: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf

[33] DoDI 5400.16: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540016p.pdf

Impact Assessment (PIA)[34]. This determination will take into account all relevant factors as presented in Section 3.2 of NIST SP 800-122 and guidance for assessing the risk of harm to individuals potentially affected by a breach in Section E of OMB Memo 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"[35].

Mission Owners will publish, collect, process and store all sensitivity levels of PII in coordination with, and with the approval of, their DoD component's senior privacy officer or their delegate.

5.1.5.1 PII at Level 2

There is a need for some low-confidentiality impact (low sensitivity) PII to be published or collected in commercial CSOs having a Level 2 PA. DoD CIO memo dated 07 August 2019, "Treatment of PII within Level 2 Commercial CSOs for DoD" states that "Level 2 will be the minimum cybersecurity requirement for DoD systems/applications containing low confidentiality impact level PII as determined in accordance with NIST SP 800-122".

Note: A DoD information impact level 2 PA is based on the FedRAMP moderate baseline, thus PII at Level 2 will be protected at the moderate level IAW 32 CFR 2002 Controlled Unclassified Information[36].

The following requirements are provided for low PII published, collected, stored or processed in commercial CSOs:

- Mission owners will only publish, collect, store and process low confidentiality impact (sensitivity) PII in a CSO minimally possessing a FedRAMP Moderate P-ATO listed on the FedRAMP Marketplace and a DoD Level 2 PA, with privacy officer approval.

- Mission owner PII impact level determination will consider all relevant factors together; one factor by itself might indicate a low impact level, but another factor might indicate a high impact level, and thus override the first factor.

- Prior to authorizing the system, the AO is accountable to review the PIA and ensure that appropriate cyber assessments are performed per DoDI 8510.01 and the CC SRG, and that required CSSP cybersecurity support services are provided per DoDI 8530.01.

- Low impact/sensitivity PII, when published or collected in a CSO with a Level 2 PA, must be minimally protected in accordance with NIST SP 800-122 and privacy laws as

[34] DD Form 2930: https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2930.pdf?ver=2017-08-11-145827-790

[35] OMB Memo 17-12: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

[36] 32 CFR 2002 CUI: https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf

supported by a FedRAMP Moderate P-ATO, and the low PII overlay of the privacy overlay (see Section *5.1.5.2, CNSSI 1253 Privacy Overlay*).

Note: Authentication and identification information of privileged users required for the configuration, operation and maintenance of the IL2 CSO and mission owner's application is exempt from the above requirements providing it is protected as all such information is customarily protected.

5.1.5.2 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*.[37] 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* [38]and *HIPAA*[39], 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 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 on which the overlay specifications are based 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 one of the best DoD resources on the subject.

This overlay addresses low, moderate and high sensitivity PII and PHI by providing an overlay for each. 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.

The CNSSI 1253 Privacy Overlay is applicable to all systems and CSOs that process or store PII/PHI for the DoD. The appropriate overlay (L, M, H, PHI) will be applied based on the confidentiality impact determination in the PIA. Mission owners wishing to process or store PII or PHI in a commercial or private CSO must apply the privacy overlay by including the CSO applicable requirements in their contracts and validate compliance for their ATO.

---

[37] Privacy Overlay: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[38] Privacy Act: http://www.archives.gov/about/laws/privacy-act-1974.html

[39] HIPAA: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html

5.1.5.3 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 E-1 – FedRAMP M C/CE Modified or Required by Regulation
  - Table E-2– 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 E-3 – *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 D-1: *FedRAMP+ Control/Enhancement Parameter Values for PA Assessment*
  - Table E-4 – *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 E-5 – *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.

5.1.5.4 CSO Assessment of Privacy Overlay Control/Control Enhancements

DISA is not assessing CSOs for privacy. Mission owners are responsible for privacy overlay assessments of the P/SaaS CSOs used and any applications built on I/PaaS.

5.1.6 Security Controls/Enhancements To Be Optionally Addressed in the Contract/SLA

Table 5-1 shows the C/CEs designated for potential inclusion in a mission owner's contract or service level agreement (SLA) with the CSP if the mission owner feels they need the added security/capability afforded by the C/CE. This is essentially a tailoring in decision 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. The SLA C/CE are CNSSI 1253 MMx C/CE that were not selected as being required as part of the FedRAMP+ C/CE set(s), however, the FedRAMP+ selection working group felt the C/CE had value if the mission owner wanted to add them to their contract. Additionally, it is the mission owner's responsibility to define any parameter values associated with any added C/CE. Typically, these values would be based on DoD RMF TAG values or CNSSI 1253 values as shown in *Table D-2.*

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 to tailor in 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 5-2: Security Controls/Enhancements Optionally Addressed in the Mission Owner's 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		
SC-18 (03)			X
SC-18 (04)		X	X
Total	9	8	9

5.1.7 Additional Considerations and/or Requirements for L4/5 DoD PA Award

The following is a list of considerations and/or requirements that must be assessed or reviewed in addition to or in conjunction with the security control assessments for AO acceptance before a Level 4/5/6 PA will be awarded. The listing may not be all-inclusive, and specific requirements may not have been fully developed at this time.

The considerations and/or requirements that DoD will assess include, but are not limited to, the following:

- How support for DoD PKI authentication by DoD privileged and non-privileged users is implemented. This is to include the processes and protocols used along with their implementation.
  - Related CC SRG sections:
    - 5.4, CSP use of DoD Public Key Infrastructure (PKI) and subsections.
    - 5.10.7, Active Directory Integration for Cloud and subsections.

- How support for DoD IP addressing will be implemented.
  - Related CC SRG section:
    - 5.10.4.1, IP Addressing. This consideration addresses any need to route commercial IP addresses across the NIPRNet
- CSP Data center locations hosting the CSO for which the PA is to be awarded.
  - Related CC SRG section:
    - 5.2.1, Jurisdiction/Location Requirements
- CSO management/monitoring plane (and/or specific devices/systems) and its integration with the CSP's corporate network or the general commercial CSO management plane.
  Note: No specifics are provided regarding this consideration at this time; however, see the next item for related concerns.
  - Related CC SRG section:
    - 5.10.2.3, Management Plane Connectivity
- CSP personnel managing and/or monitoring the CSO infrastructure. This is primarily related to U.S. persons constraints in regard to the previous item.
  - Related CC SRG section:
    - 5.6.2, CSP Personnel Requirements.
- The availability of a private connection capability between the off-premises CSP's/CSO's network and DoD networks in support of connections through the boundary cloud access point (BCAP) and meet-me points.
  - Related CC SRG section:
    - 5.10.1, Cloud Access Point (CAP) and subsections.
    - 5.10.1.1.2, NIPRNet BCAP Meet-Me Points
    - 5.10.1.1.3, CSP Support for BCAP Connectivity
- Reliance of the CSO or user experience on internet-based capabilities such as the public DNS or content delivery networks. All such capabilities must be available via the CSO infrastructure and the connections to it via the DISN BCAPs. The CSO must be able to function if DoD limits access to or disconnects from the internet in times of conflict or when the DISN/DODIN is being attacked.
  Note: No specific requirements other than those noted here are provided.
  - Related CC SRG section:
    - 5.10.4.2, Domain Name Services (DNS).
- Reliance on internet access to reach the CSO management/service-ordering portal or API endpoints from either NIPRNet or from within the CSO. All such access must be via the CAP if from the NIPRNet or must remain on the CSP's/CSO's network if from within the CSO. These requirements must be minimally configurable if not inherent.
  Note: No specific requirements other than those noted here are provided.
  - Related CC SRG section:
    - 5.10.1, Cloud Access Point (CAP) and subsections.
- The protections in place in the CSP's network and CSO to prevent any internet connection to the CSP's/CSO's network and CSO from becoming a back door to the NIPRNet via the private connection through the BCAP.
  - Related CC SRG section:
    - 5.10.1.1.4, CSP/CSO Network Connectivity to internet and BCAP.
- The robustness of the CSP's required boundary protection (defense-in-depth security/protective measures) implemented between the internet and the CSO for its

protection from internet-based threats. This protection is expected to be different depending on whether the CSO is I/PaaS or P/SaaS and whether the Mission Owner has control over their portion of the CSO.
    - Related CC SRG section:
        - 5.10.3, CSP Service Architecture and subsections.
- All other requirements as defined in the rest of this SRG
- Other considerations as realized while assessing the CSO or as a result of lessons learned.

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 U.S. government data can be processed/stored. This is nuanced by the information being on DoD premises.

To protect against seizure and improper use by non-U.S. 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 U.S. This may include DoD bases on foreign soil depending upon Status of Forces Agreements (SOFAs). 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 U.S. (as defined at FAR 2.101[40]), 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. Additionally, the mission owner and/or contracting officer must review CSP terms and conditions to ensure data stored and processed in U.S. datacenters does not fall under the legal jurisdiction of another country.

On-premises CSOs implemented by a DoD or non-DoD CSP which uses a hybrid model employing off-premises CSPs and CSOs to augment the on-premises CSO or by virtually extending the DoD fence-line (DISN boundary) must also meet the location requirements stated here. **Note:** An exception is made for content delivery networks (CDN) in which non-sensitive DoD data may be cached anywhere in the world. However, when sensitive information is requested through a CDN, the request must be sent back to its storage facility under U.S. jurisdiction for retrieval.

Corresponding Security Controls: SA-9(5)

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

5.2.1.1 DoD Off-Premises vs. On-Premises vs. Virtually On-Premises

DoD on-premises vs. off-premises relates to the physical or virtual location of a facility or IT infrastructure.

DoD off-premises: A facility (building/container) or IT infrastructure is off-premises if it is NOT physically or virtually on DoD owned or controlled property (i.e., on-premises). Refer to DoD on-premises and DoD virtually on-premises below.

DoD on-premises: A facility (building/container) or IT infrastructure is on-premises if it is physically on DoD owned or controlled property. That is, it is within the protected perimeter (walls or "fence line") of a DoD installation (i.e., base, camp, post, or station (B/C/P/S) or leased commercial space) which is under the direct control of DoD personnel and DoD security policies.

DoD on-premises includes DoD data centers, other facilities located on a DoD B/C/P/S, or in a commercial or other 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. Such facilities are considered to be within the protected perimeter or "fence line" of a DoD controlled installation or property. Physical facilities may be permanent buildings or portable structures such as transit/shipping containers. An example of the latter might be a shipping container housing a commercial CSP's infrastructure located adjacent to a core data center and connected to its network as if it were inside the building.

DoD CSPs will, and commercial CSPs may (under DoD contract), instantiate their CSO 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.

DoD virtually on-premises: A DoD private IT and/or CSO infrastructure located in a physically off-premises location (facility) such as a federal government or commercial data center (i.e., facilities under the direct control of non-DoD personnel using non-DoD security policies) may be considered virtually on-premises under specific conditions as listed below. These conditions apply certain physical security controls and extend the DISN accreditation boundary. In essence this construct virtually extends the DoD protected perimeter or "fence line" around the infrastructure. It also places the IT/CSO infrastructure and its management plane in one or more DISN enclaves thus enabling alternative approaches for boundary protection such as using CSO provided infrastructure in lieu of a dedicated DoD ICAP/BCAP.

An IT/CSO infrastructure may be considered virtually on-premises under the following conditions:

- The CSO infrastructure is DoD private/community and its infrastructure, devices, monitoring/support infrastructure, and management plane are dedicated to it; physically separate from other infrastructure, devices, and network enclaves in the data center.

- DISN transport is extended to the CSO's network enclave(s) supporting the CSO infrastructure, CSO monitoring/support infrastructure, and CSO management plane.

- Enclave/datacenter boundary protections are implemented to protect the CSO operational enclave(s) (which may include the CSO monitoring/support infrastructure) IAW DISN enclave boundary or core data center protection requirements.

- The CSO infrastructure is managed from one or more enclave(s) dedicated to managing the CSO. This can be done using dedicated workstations in the enclave or remotely using dedicated virtual desktop infrastructure (VDI).

- Enclave boundary protections are implemented to protect the dedicated CSO management/monitoring/support enclave(s) IAW DISN enclave boundary protection requirements.

- The CSO infrastructure is housed in a physically separate/protected space such as a cage or room (or minimally one or more locked cabinets with closed non-removable sides closing the DoD space) within the commercial data center used to house the DISN network device(s) and CSO infrastructure. Related C/CE: PE-3, PE-3(1)*, PE-3 (4)*, PE-4

- This physically separate space is minimally protected as follows:

    - Physical access to the data center is compliant with all required physical and maintenance personnel access security controls in the FedRAMP moderate or high baseline as appropriate to include but not limited to personnel role-based access control, access auditing, visitor access control and escorting as needed, etc. Related C/CE: MA-5, MA-5(1), PE-2, PE-2 (3)*, PE-3, PE-3(1)*, PE-6, PE-6(1). PE-6(4)*, PE-8,

    - Physical access to the DoD space is compliant with all required physical and maintenance personnel access security controls in the FedRAMP moderate baseline or high baseline as appropriate (as described above for the data center) and/or appropriate CNSSI 1253 baselines.

      NOTE: Additional or alternate physical security and personnel controls may be required for facilities housing classified systems.

    - Personnel access is controlled by an automated entry access control system (AECS) that is token and/or biometric based. This system may be under DoD control or under the control of the facility owner, but must limit access to only authorized individuals, must log/audit all accesses to include the identities of the personnel accessing and departing, and must provide and log alerts for unauthorized accesses and failed attempts. Related C/CE: PE-6, PE-6(1) and PE-6(4)*

    - Access to the physical space is externally monitored by the facility owner using video cameras and physical intrusion detection system (PIDS) (i.e., intrusion alarm system). Related C/CE: PE-6, PE-6(1), PE-6(3)*, and PE-6(4)*

    - It is highly recommended that the internal space be monitored by an automated motion activated PIDS and video cameras operated by DoD. In this manner DoD can

monitor all physical activities within the space, authorized or unauthorized. Related C/CE: PE-6, PE-6(1), PE-6(2)*, PE-6(3)*, and PE-6(4)*

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 community). A private cloud service implements dedicated infrastructure to serve one customer organization or community. 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 multiple 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 (DoD community) 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 level 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 federal government community or DoD private/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 federal government community or DoD private/ 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.

Note: While multi-tenant CSOs marketed as ITAR compliant", "government clouds", or "clouds for government" might restrict data location to U.S. jurisdiction, and might restrict the personnel that manage the CSO, 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 U.S. 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.

5.2.2.3.1 Impact Level 5 Separation in an Impact Level 4 CSO

Sufficient separation of compute and storage for level 5 systems and data may be optionally achieved in a level 4 CSO under certain circumstances. CSPs may wish to offer a level 5 CSO in a larger level 4 CSO possessing a DoD PA. The level 5 CSO is based on a subset of services offered by or in addition to the level 4 CSO. The specific minimum requirements are as follows:

- The supporting CSO must have a level 4 PA. A separate level 5 PA with conditions addressing the core services enabling the separation and approved supporting services will be developed.
- Physical compute platforms must be dedicated to the mission owner's system.
  - The CSO must offer one or more services that permit the mission owner to select dedicated compute platforms under their account.
  - The mission owner must select one or more of the dedicated platform services for their system's account and operations.
- All data related to the level 5 system must be encrypted at rest within the CSO and related CSOs. This includes DoD information processed, stored, or transmitted by the system, as well as the system's virtual hard drives.
  - Encryption keys must be in the control of the mission owner with no or tightly restricted access by CSP personnel. Only the mission owner's systems may be able to decrypt the data.
  - Encryption modules must be FIPS 140-2 or FIPS 140-3 validated and operated in FIPS Mode or implement other NSA approved cryptography.
- NSA must evaluate and provide a risk assessment on any key management systems (KMS). CSOs supporting the cryptography requirements with a focus on cryptography operations and key management. Refer to Section *5.2.2.3.1.1 Cloud-Based KMS Security Requirements* for minimum KMS security requirements and additional engagement information. This is in addition to 3PAO assessment of the overall Level 4 and 5 CSOs.

Note: While the requirements here are primarily focused on an IaaS CSO, they are also applicable to PaaS and SaaS CSOs. Additional requirements may be necessary for these CSOs.

CSPs having a Level 4 PA wishing to offer a CSO as described here should contact the DISA Cloud Support Office. DISA will engage NSA, and NSA will then establish a contractual arrangement with the CSO to affect the risk assessment.

5.2.2.3.2 Cloud-Based KMS Security Requirements

This section addresses security requirements that a cloud-based KMS must satisfy for protecting IL5 information in an IL4-accredited cloud.

NSA shall be responsible for evaluating a cloud-based encryption and KMS for use as a solution to protect IL5 information in an IL4-accredited cloud according to the following requirements:

1. The CSP shall protect IL5 information using cryptographic algorithms and key sizes selected from the Commercial National Security Algorithm (CNSA) suite.

   Note: The Commercial National Security Algorithm (CNSA) replaced Suite-B in specifying NSA preferred algorithms and key sizes for protecting information up to Top Secret.

2. Cryptographic algorithms and protocols used in the cloud-based KMS shall be implemented according to applicable cryptographic standards.

   a. Cloud-based KMS components shall have been evaluated against and determined to be compliant with applicable National Information Assurance Partnership (NIAP) Protection Profiles.

   b. Cryptographic software modules used in cloud-based KMS shall have received FIPS 140-2 or FIPS 140-3 accreditation.

   c. Cryptographic hardware security modules used in cloud-based KMS shall have received FIPS 140-2 or FIPS 140-3 Level 3 accreditation.

Note: FIPS 140-3 became effective on September 22, 2019. FIPS 140-3 testing will begin on September 22, 2020. Before September 22, 2020 cryptographic modules shall be evaluated against FIPS 140-2; September 22, 2020 and after cryptographic modules shall be evaluated against FIPS 140-3.

3. Cryptographic algorithms, protocols, and procedures used in cloud-based KMS shall be developed and maintained in accordance with a secure software development lifecycle process.

Note: Recognizing that software will always tend to contain vulnerabilities, secure code lifecycle processes help to detect and remove vulnerabilities from code during and after development.

4. The DoD mission owner shall control the keys used to protect that mission's information:

   a. The CSP shall provide secure methods for managing access to a mission's keys and information.

   b. The CSP shall securely delete a mission owner's keys on demand from the mission owner.

      i. If the CSP makes deleted keys recoverable by default, the CSP shall inform the mission owner how long a key will be in a recoverable state.

      ii. The CSP shall provide the mission owner with the ability to make keys unrecoverable when deleted. The mission owner shall accept the risk that the keys will no longer be available.

Note: CSPs commonly make deleted keys recoverable for a short period of time in case the customer discovers that deleting a key was done by mistake.

c. The CSP shall provide the customer with secure methods for importing keys into the cloud and for exporting keys from the cloud.

5. The CSP shall have security procedures in place to prevent CSP personnel from gaining access to customer keys:

   a. The CSP shall encrypt customer keys while at rest in the cloud.

   b. The CSP shall protect customer keys using secure channels when the keys are transmitted internally to the cloud system.

   c. The CSP shall minimize the exposure of customer keys while the keys are being actively used for cryptographic purposes.

      i. The CSP shall ensure only the cryptographic process required to use an unencrypted key shall have access to the key;

      ii. The CSP shall ensure an unencrypted key is not stored in memory longer than necessary.

      iii. The CSP shall ensure an unencrypted key is securely deleted from memory and disk when no longer needed.

   d. The CSP shall have processes in place to detect malicious administrators or other inside attacker activities.

6. The CSP shall ensure cryptographic processes that handle customer keys are securely separated from other processes.

Note: Cryptographic processes are considered to be properly separated if they do not intermingle customers' key material and a vulnerability in a key relevant process does not compromise the security of other customers' keys.

5.2.2.3.3 NSA Cloud-Based KMS Evaluation Methodology

NSA will evaluate a cloud-based KMS against the security requirements detailed in this document by performing the following activities:

1. Engagement with the CSP to gain insight into details about the architecture and cryptographic services that are relevant and cannot be gained by public literature;

2. Analysis of the cloud-based KMS or documentation from the vendor regarding detailed operation of these services;

3. Security analysis of the web tier to assess security posture against web vulnerabilities, such as incorrectly implemented access controls, common web vulnerabilities, or other

attacks that could be used to compromise an account. Enumeration of controls in place to defend against such attacks;

4. Analysis of the cloud architecture to determine how vulnerabilities in the architecture could allow malicious actors to gain access to DoD data or keys;

5. Confirmation that the cloud vendor has relevant government certifications, FIPS validations, and NIAP Protection Profiles.

Direct platform testing shall be the preferred method for evaluating requirements, but vendor attestation shall be acceptable when direct platform testing is not feasible. Methods used to evaluate each requirement shall be documented and considered when developing a risk recommendation for the cloud-based KMS solution.

5.2.2.3.4 Process of Requesting a Cloud-Based KMS Evaluation from NSA

To request an evaluation of a cloud encryption and key management system, the DoD shall enter a Customer Service Request Portal (CSRP) request to NSA, specifically requesting this type of evaluation in support of the DoD CCSRG. The DoD shall direct the request to the Office of the National Manager (ONM), who will then task the appropriate NSA organizations in the Cybersecurity Directorate (C1 - Analysis and Mitigations and C2 - Encryption Production and Solutions) to perform the evaluation. The length of the evaluation shall be no shorter than three months. After the evaluation is complete, C1 and Y2 will produce documentation about the evaluation and provide a risk recommendation.

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. Refer to Section 6.5.4*, 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

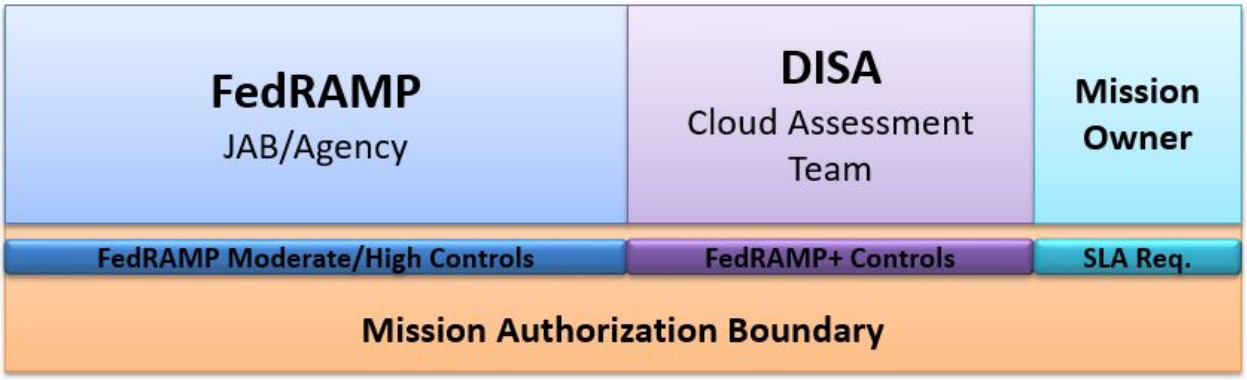
5.3 Ongoing Assessment

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* [41]and *FedRAMP Continuous Monitoring Strategy Guide.*[42] 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 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 assessment responsibility is shown in Figure 5-1.

Figure 5-1: Ongoing Assessment Division of Responsibility



[41] Guide to Understanding FedRAMP: https://www.fedramp.gov/resources/documents/

[42] FedRAMP Continuous Monitoring Strategy Guide: https://www.fedramp.gov/resources/documents/

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, *Cyberspace 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 Figures 5-2, 5-3, and 5-4, 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 use 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[43], August 3, 2015. Additional information regarding this format can be found at www.niem.gov.

All FedRAMP provisionally authorized 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. This means DoD will leverage and use the FedRAMP Continuous Monitoring (CONMON) process and artifacts to the greatest extent possible. CSOs in the FedRAMP catalog will follow the process described in the *FedRAMP Continuous Monitoring Strategy Guide*[44]. 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

[43] DoDI 8320.07: http://www.dtic.mil/whs/directives/corres/pdf/832007p.pdf

[44] FedRAMP Continuous Monitoring Strategy Guide: https://www.fedramp.gov/resources/documents/

5.3.1.1 Continuous Monitoring for CSOs in the FedRAMP Catalog with a DoD PA

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. DoD leverages the CSOs CONMON artifacts and the work done by the FedRAMP TRs in which DoD is a part of the team.

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 cybersecurity service providers (CSSPs).

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 5-2 shows the normal flow of continuous monitoring information if the CSP has a FedRAMP JAB PA.

Figure 5-2: DoD Continuous Monitoring for CSOs with a FedRAMP JAB PA

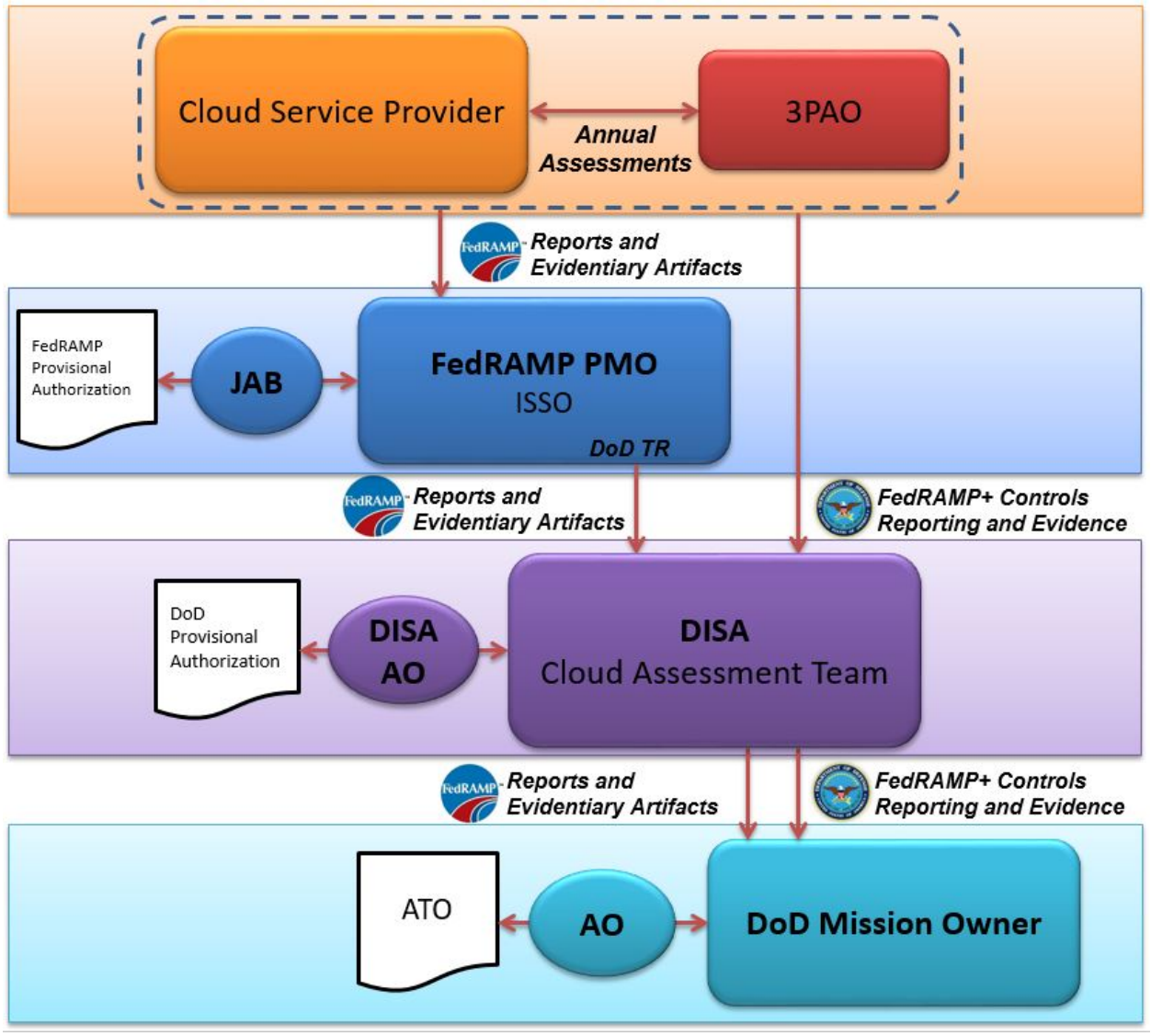
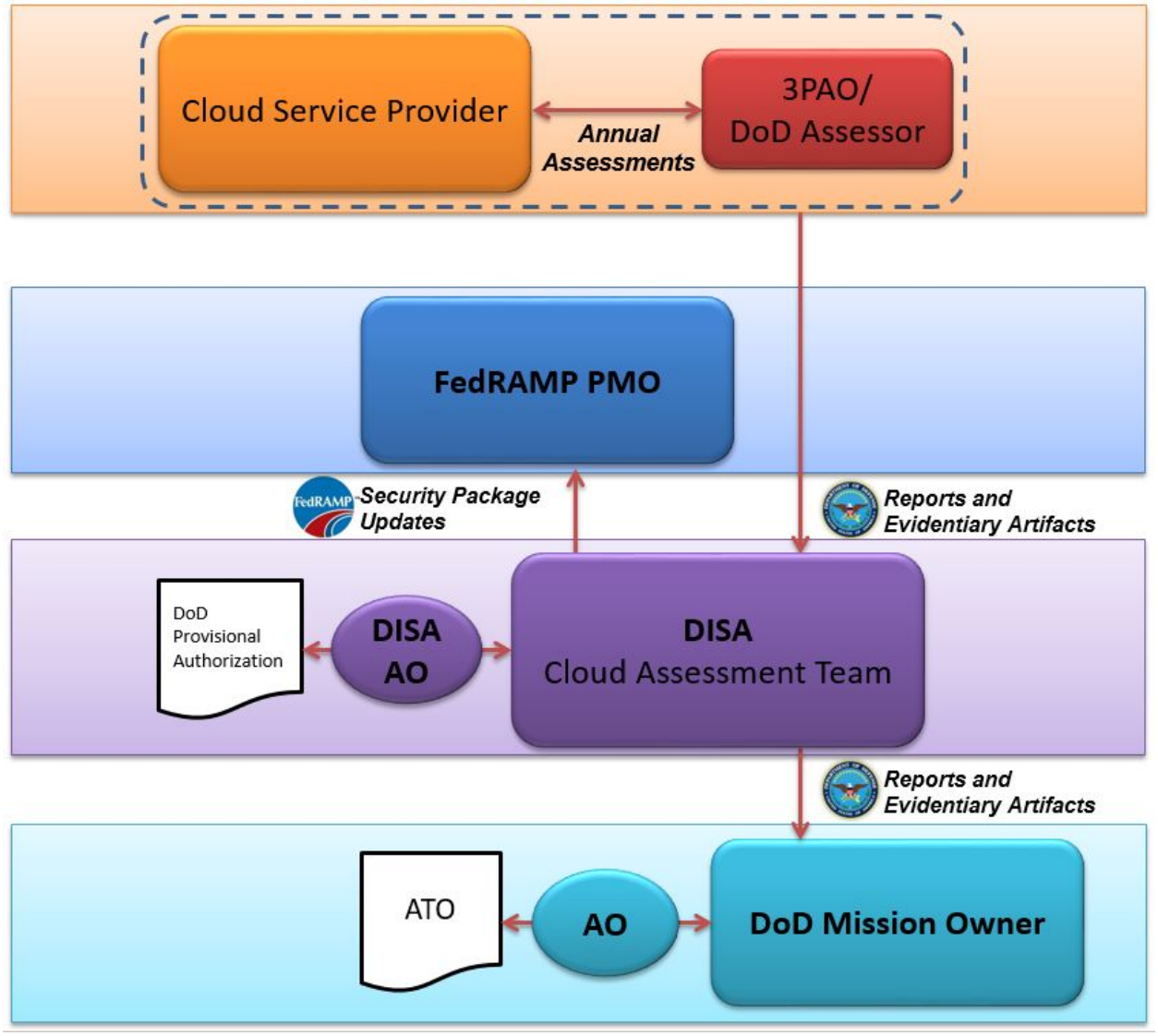


Figure 5-3 shows the flow of continuous monitoring information if the CSO has a 3PAO assessed non-DoD Federal Agency ATO listed in the FedRAMP catalog. Since the FedRAMP JAB does not control the Agency ATO, information may not flow from the CSP to the FedRAMP PMO.

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

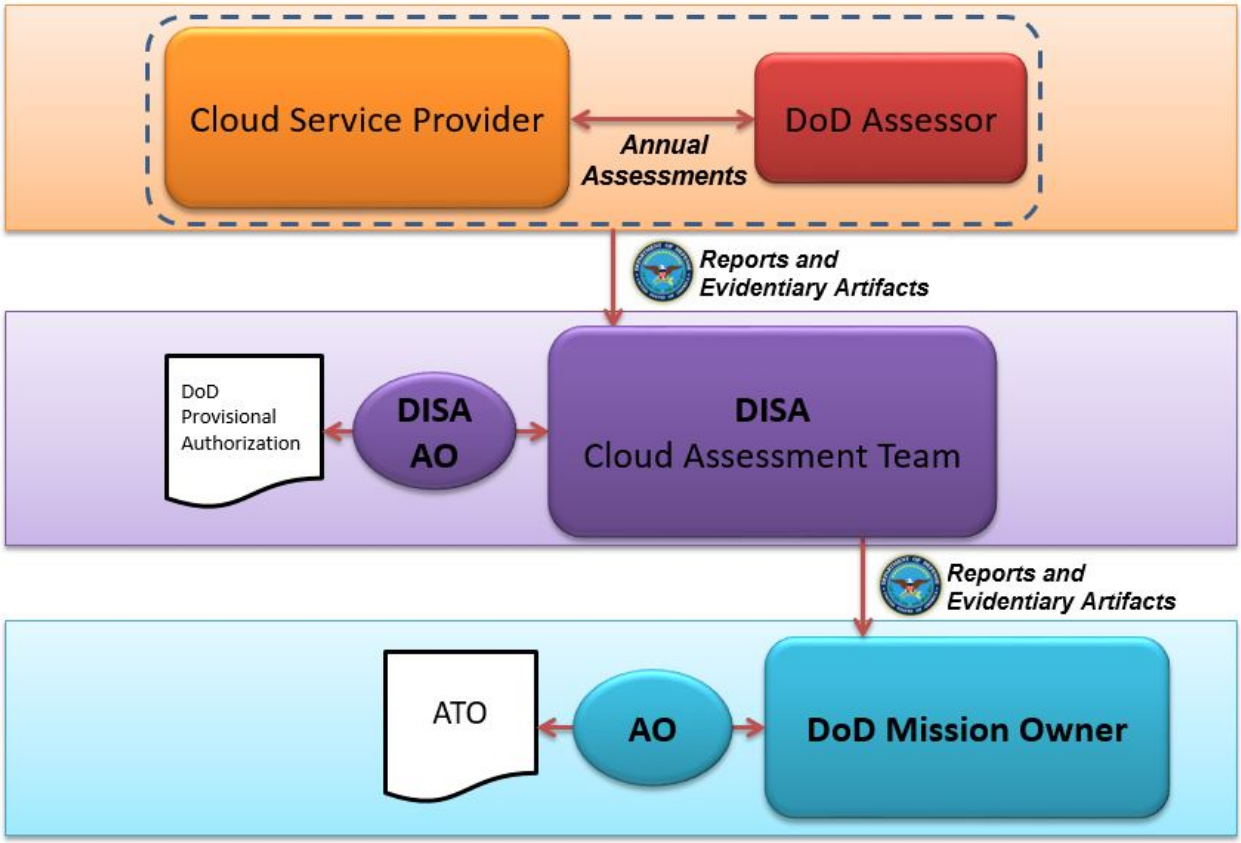


5.3.1.2 Continuous Monitoring for DoD Assessed CSOs

Figure 5-4 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 cybersecurity service provider (CSSP) entities as defined in Section 6, *Cyberspace Defense and Incident Response.*

.

Figure 5-4: DoD Continuous Monitoring for DoD Assessed CSOs



5.3.2 Change Control

The DoD change control process for CSOs mirrors and leverages 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 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 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 5-5, Figure 5-6, and Figure 5-7 show these change control processes.

Note: NIST SP 800-37 Revision 1, Appendix F February 2010[45] defines a significant change as follows: "a change that is likely to affect the security state of an information system." Examples are provided as follows: "Significant changes to an information system may include for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations."

Corresponding Security Controls: CM-3, CM-4, CA-6

5.3.2.1 Change Control for CSOs in the FedRAMP Catalog with a DoD PA

The FedRAMP Continuous Monitoring Guide defines a significant change as a change to the scope of an approved PA or an impact to the authorization boundary of the CSO. The CSP will follow procedures defined in the continuous monitoring strategy guide by submitting a FedRAMP *Significant Change Security Impact Analysis Form*[46] to the FedRAMP PMO. The review of the security implications of significant changes will be performed at multiple layers, as reflected in Figure 5-5. The planned change will be reviewed by the FedRAMP ISSO and/or JAB technical representatives (TRs), and then forwarded to the JAB for approval. Simultaneously the DoD JAB TR will notify DISA, who will in turn notify all mission owners utilizing that CSO, the DISA AO, and the CSSP entities as defined in Section 6, *Cyberspace Defense and Incident Response.* During FedRAMP ISSO review, the DoD JAB TR will collect comments from DoD stakeholders and inform the FedRAMP ISSO if planned changes will adversely affect the security of the information hosted by the CSO for DoD cloud customers. DoD may communicate directly with the CSP and their 3PAO regarding change approval or concerns over the impact on DoD's FedRAMP+ C/CEs.

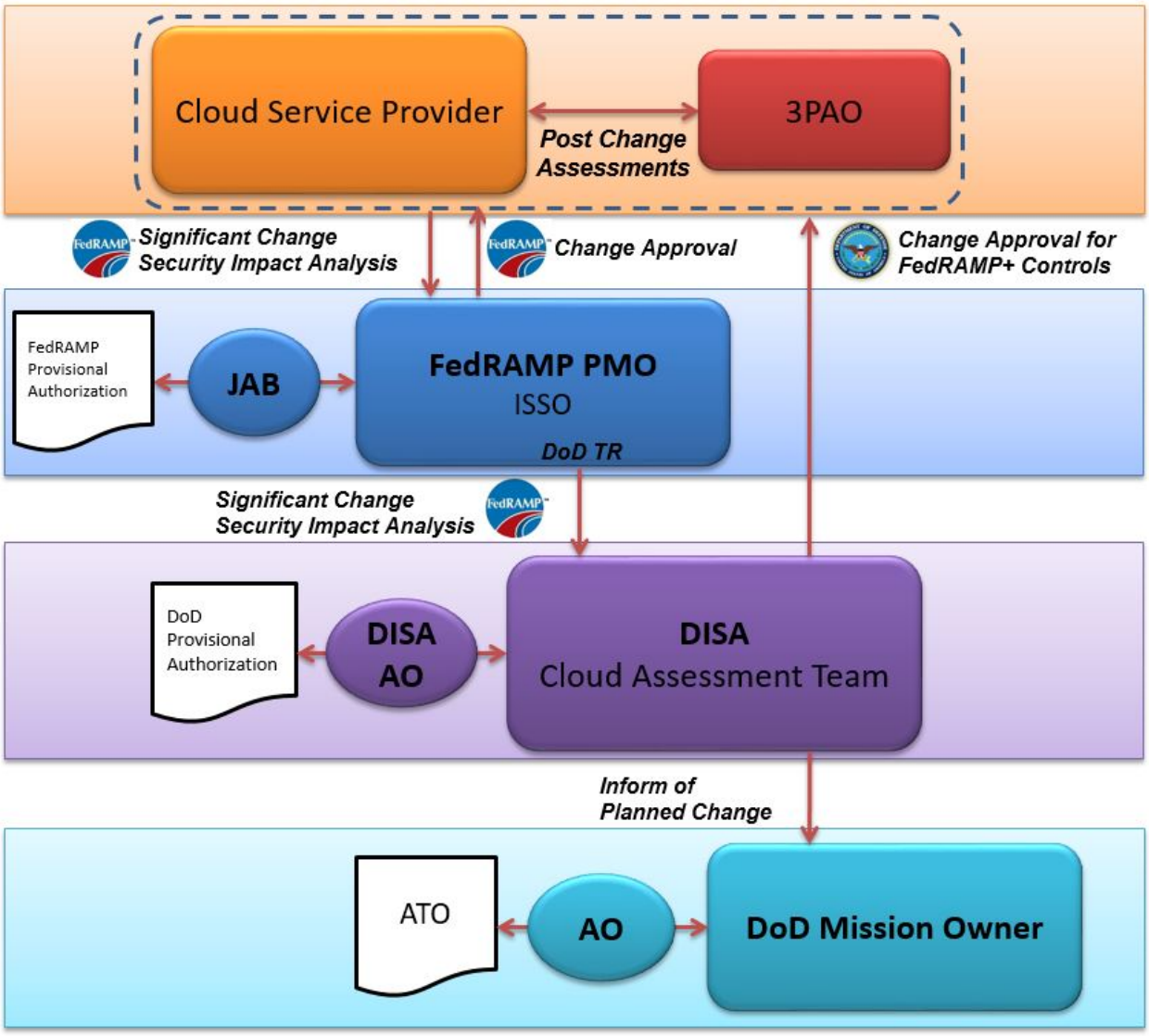
FedRAMP requires a security assessment be performed by a 3PAO after a significant change is implemented, with a corresponding security assessment report created. CSPs must also include all FedRAMP+ C/CEs in post-change assessments to meet DoD requirements. DISA will notify affected mission owners of proposed 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.

[45] NIST SP 800-37: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[46] Significant Change Form: https://www.fedramp.gov/files/2015/03/Significant_Change_Form_110812.doc

Figure 5-5 shows the normal flow of significant change information if the CSP has a FedRAMP JAB PA.

Figure 5-5: DoD Change Control Process for CSPs CSOs with a FedRAMP JAB PA

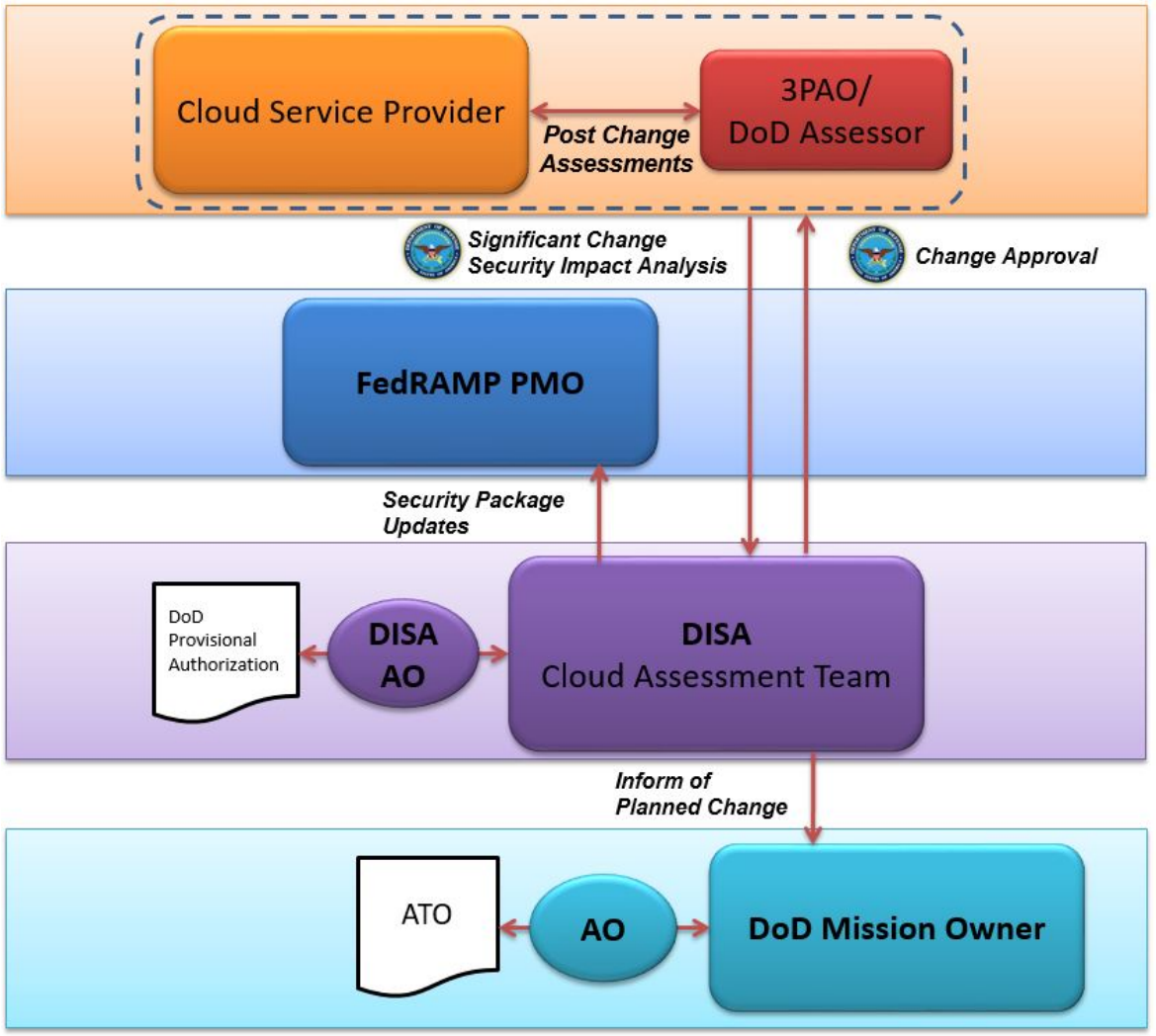


When a CSO having a DoD PA is included in the FedRAMP catalog, but does not have a JAB PA, the CSP will notify DISA directly in addition to any other required points of contact. (e.g., A CSP with a non-DoD agency ATO would notify both that agency and DISA). This is required because the FedRAMP JAB does 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 CSSP entities as defined in Section 6, *Cyberspace 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 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.

As with FedRAMP, DoD requires a security assessment be performed by a 3PAO after a 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 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 5-6 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.

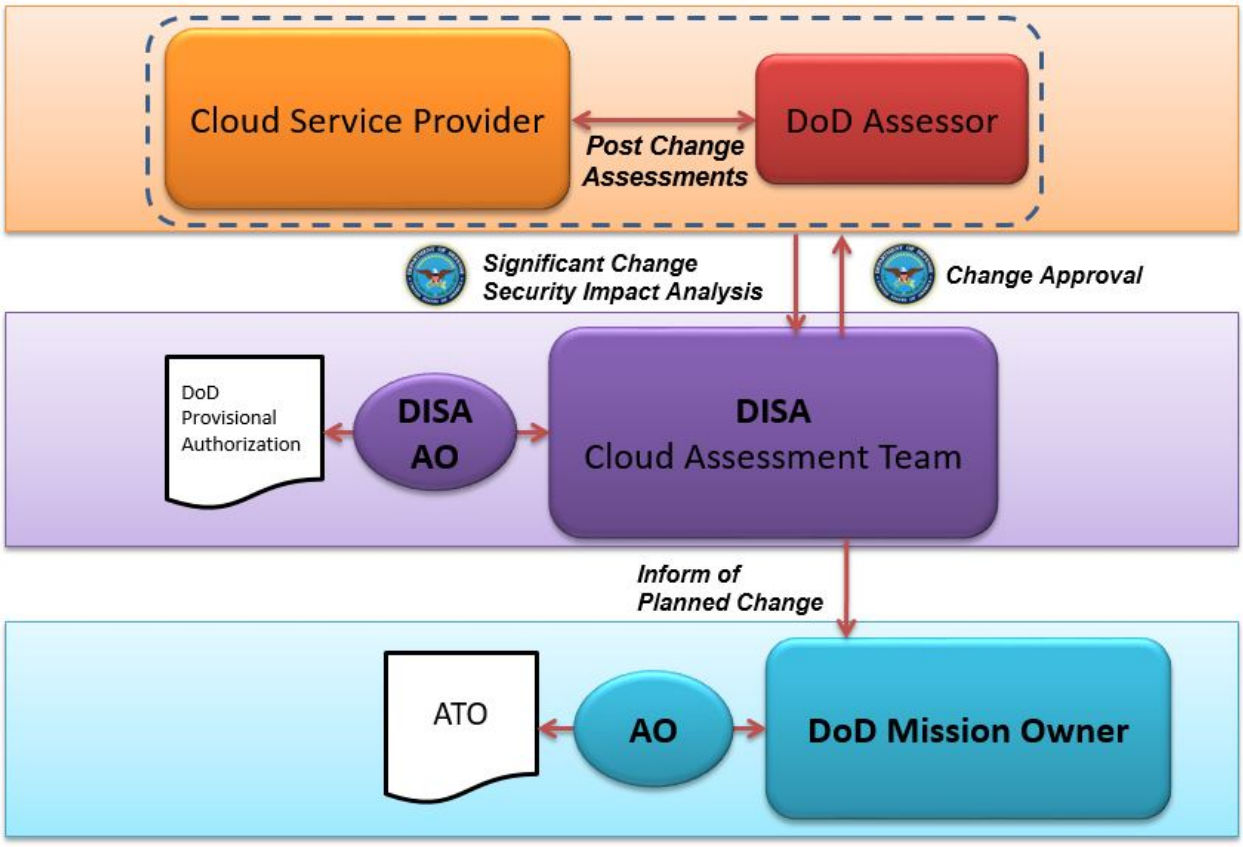
Figure 5-6: DoD Change Control Process for FedRAMP CSPs CSOs with a 3PAO Assessed Federal Agency ATO



5.3.2.2 Change Control for DoD Assessed CSOs

Figure 5-7 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 CSSP entities as defined in Section 6, *Cyberspace 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 5-7: DoD Change Control Process for DoD Self-Assessed CSPs/CSOs



5.3.3 Support for Financial Audits – SOC 1 Type II Reports

The 20 May 2019 DoD CIO Memo titled *System and Organization Control Report Requirement for Audit Impacting Cloud/Data Center Hosting Organizations and Application Service Providers* stipulates that CSPs and their subcontractors provide annual System and Organization Control (SOC 1) Type II reports in support of DoD financial audits. DoD mission owners must add this requirement to their contracts with the CSPs. Mission owners and CSPs must refer to the memo and its "Attachment A" for details of fulfilling the requirement.

Note: Cloud/data center hosting organizations is interpreted here as CSPs providing IaaS CSOs while application service providers (ASPs) is interpreted here as CSPs providing PaaS/SaaS CSOs. In both cases, the contracted CSP must obtain and provide reports from any and all subcontractors (e.g., data centers and CSP's hosting their CSO infrastructure) and from any CSPs whose CSOs the contracted CSP (ASP) is leveraging as an external service to provide their complete CSO.

As a condition of receiving a DoD PA, CSPs must demonstrate they have the ability to meet the requirement to produce SOC 1 Type II reports as stipulated in the memo and attachment for themselves and for any subcontractors and to coordinate the time period with the federal government's fiscal year.

The memo and attachment are included here for the reader's convenience; however, the mission owner and CSP should refer to the memo found at the link in the footnote to ensure there have been no changes since the publication of this release of the CC SRG.

The memo is as follows:

Beginning fiscal year 2018, the Department of Defense (DoD) is under full annual financial statement audits. In support of these audits, DoD components are directed to obtain annual SOC 1 Type II reports from cloud/data center hosting organizations and application service providers (ASPs) hosting or delivering financial or non-financial applications that impact internal controls relevant to multiple DoD financial statement audits. DoD components should work with their financial and contract personnel to determine if their cloud/data center hosting organization or ASP is affected and to ensure service organizations and relevant sub-service organizations submit SOC 1 Type II reports in accordance with requirements in Attachment A. In those instances where only a single DoD audit is impacted, and alternate solution is the inclusion of a right to audit clause in relevant service organization contracts.

Attachment A

System and Organization Control (SOC 1) Type II

Reporting Requirements for Service Organizations

The following are SOC 1 Type II reporting requirements to address the specific needs of Department of Defense (DoD) financial statement auditors where service organizations are providing audit impacting platform or infrastructure as a service (cloud/data center hosting services) and/or software as a service (application service providers).

<u>Cloud/Data Center Hosting Organizations and Application Service Providers (ASPs)</u>

1. The SOC 1 report must be prepared in accordance with the following auditing standards:
   - Attestation Standards Clarified (AT-C) Section 320, "Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting"
   - AT-C Section 105, "Concepts Common to All Attestation Engagements"
   - AT-C Section 205, "Examination Engagements"

2. The SOC 1 report must address the design and operating effectiveness of the service organization's controls to meet identified control objectives (generally referred to as a Type II report).
3. The SOC 1 report will include information system general control objectives that are comparable with the U.S. Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM) control objectives for security management, access controls, configuration management, segregation of duties, and contingency planning.
4. The SOC 1 report period will begin October 1 and end on June 30 of each year.
5. The SOC 1 report will be delivered to DoD (FIAR directorate) no later than August 15 of each year.
6. The service organization will provide a bridge letter to DoD no later than October 8 of each year to address the period from July 1 through September 30.

Incremental Requirements for ASPs

In addition to the requirements for cloud/data center hosting organizations, SOC 1 reports for ASPs will include the following incremental requirements for relevant application(s).

1. The report will include business process application control objectives that are comparable with the GAO FISCAM control objectives for the completeness, accuracy, and validity of inputs, processing, outputs, and master data.
2. The SOC 1 report will identify key inputs and the service organization's rationale and approach for identifying the key inputs.
3. The SOC 1 report will identify inbound/outbound interfaces and the service organization's rationale and approach for identifying the key interfaces.
4. The SOC 1 report will identify automated data/transaction edits and the service organization's rationale and approach for identifying the key edits.
5. The SOC 1 report will identify key outputs/reports and the service organization's rationale and approach for identifying the key outputs/reports.

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 in to for configuring 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 NSS 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[47] while the Federal PKI is operated by GSA[48]. 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

[47] DoD PKI/PKE: http://iase.disa.mil/pki-pke/Pages/index.aspx

[48] Federal PKI: http://www.idmanagement.gov/federal-public-key-infrastructure

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.

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 5-3 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 5-3: 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 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.	▪ Non-privileged user access to non-publicly released non-CUI and non-critical mission information in the CSP's SaaS offering 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., two-factor token-based onetime password, DoD-approved[49] 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[50].	▪ 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[51].

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

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

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

Impact Level	Implemented by Mission Owner IAW DoD Policy	Implemented by CSP IAW FedRAMP's selection of IA-2(12)
	▪ 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.	▪ 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 to administer mission owner systems/applications instantiated on IaaS/PaaS requires the use of NSS SIPRNet Token/PKI.	▪ 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' 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 use an assertion service that is compliant with DoD standards. An assertion service is a DoD strong authentication mechanism that provides additional challenges and responses to prove an identity IAW *DoD Cybersecurity Discipline Implementation Plan, October 2015, Amended February 2016*[52]. An example of this is a two-step verification where an access code is sent to the user via a different communications path than the one accessing the website 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.

[52] DoD Cybersecurity Discipline Implementation Plan, October 2015, Amended February 2016; https://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf

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 Cyber Exchange website page Public Key Infrastructure (PKI) and Public Key Enabling (PKE)[53] provides information needed to PK-enable mission owner's systems/applications

[53] DoD PKI/PKE: http://iase.disa.mil/pki-pke/Pages/index.aspx

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 use 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 Cyber Exchange website[54] along with an SRG/STIG Applicability Guide[55].

DoD recommends that STIGs and/or SRGs be used by CSPs 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 by CSPs is preferable, industry standard baselines such as those provided by the Center for Internet Security (CIS) benchmarks are an acceptable alternative to the STIGs and SRGs.

Impact levels 4/5/6: STIGs are applicable if the CSP uses 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. While the DoD level 4/5/6 value for CM-6 is to use DoD SRGs and STIGs as applicable, DISA will evaluate the CSP's usage of commercial equivalencies (e.g., CIS benchmarks) on a case-by-case basis.

For dedicated infrastructure that only serves DoD tenants, CSPs must use 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

[54] STIGs and SRGs: http://iase.disa.mil/Pages/index.aspx

[55] SRG/STIG Applicability Guide: http://iase.disa.mil/stigs/agct/Pages/index.aspx

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*[56].

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 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 U.S. citizens or non-citizen U.S. nationals as defined in 8 U.S. Code § 1408[57], national affiliation is defined in 22 CFR 120.15[58] – U.S. person and 120.16 – foreign person.

The limitations by information impact level are as follows:

---

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

[57] 8 U.S. Code § 1408: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title8/pdf/USCODE-2010-title8-chap12-subchapIII-partI-sec1408.pdf

[58] 22 CFR 120.15, 120-16: https://www.gpo.gov/fdsys/pkg/CFR-2011-title22-vol1/pdf/CFR-2011-title22-vol1-sec120-15.pdf

Impact level 2: CSP personnel having access to the systems processing/storing DoD public information may be U.S. citizens, U.S. nationals, U.S. 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 level 4/5 must be U.S. citizens, U.S. nationals, or U.S. 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 U.S. 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 Tool*[59] is 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 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

[59] OPM Position Designation Tool: https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/

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 DoDM 5200.02, *Personnel Security Program*[60] 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 ensure 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[61], an agency must stipulate, "IAW OPM and OMB requirements," the type of background investigation required for CSP personnel having access to 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 with Law and Credit (NACLC). The position

[60] DoDM 5200.02: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002m.PDF

[61] FedRAMP Control Specific Contract Clauses v2, June 6, 2014; http://cloud.cio.gov/document/control-specific-contract-clauses

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 DoD systems and/or data. Personnel who have access to the CSP infrastructure only (i.e., at the hypervisor or below for IaaS or PaaS/SaaS CSO applications and below without access to DoD customer systems or data) 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 website.[62] 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 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

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

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[63] and the IAW DoDM 5200.02[64], both entitled *DoD Personnel Security Program (PSP)*. Commercial CSPs' personnel clearances are granted through the Industrial Personnel Security Clearance Process[65].

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[66] and Federal Acquisition Regulations (FAR) Section 52.204-2 - Security Requirements[67]. 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[68], also states the following: "Agencies leveraging FedRAMP Provisional Authorizations will be responsible for conducting their own Background Investigations and or accepting reciprocity

---

[63] DoDI 5200.2: http://www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf

[64] DoDM 5200.02 : https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002m.PDF

[65] Industrial Personnel Security Clearance Process: http://www.dss.mil/psmo-i/indus_psmo-i_process_applicant.html

[66] 48 CFR Subpart 4.4:

https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4-subpart4-4

[67] FAR 52.204-2:

https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf

[68] FedRAMP Control Specific Contract Clauses v2, June 6, 2014; https://www.fedramp.gov/resources/documents/

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. Additionally, mission owners may require that some CSP personnel have clearances in the event classified information sharing may be needed at some point in time. This may be based on the criticality of the CSO's use case and the criticality or type of information. DoD components and/or mission owners must review the investigation type required for all position designations and address investigation requirements and any clearance 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[69] 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*[70], 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 6.5 *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 in traditional IT are typically remediated or "cleaned" by sanitizing affected hardware to ensure that

[69] DoD 8570.01-M: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

[70] CNSSI 4009: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

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 or impossible 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.

Where the mission owner has control over the cloud environment and/or how their data is stored as in IaaS and some PaaS CSOs, 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 read. Additionally, file deletion will most likely ensure the file's location will be overwritten with new data. This will typically happen quickly in a high use cloud environment. CE coupled with file deletion 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 use 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.

Where the mission owner does not have control over the cloud environment and/or how their data is stored as in most SaaS and some PaaS CSOs, the CSP must provide capabilities within the CSO that can be activated when a spillage is detected. These capabilities should be under the

control of the mission owner. Granular DAR encryption and data deletion capabilities at the file or database record/field level along with Crypto Erase should be part of such capabilities.

CSPs must provide a spillage remediation plan based on their various and specific data storage systems and processes addressing the above and mission owner control of capabilities for all CSOs as part of their provisional authorization package. This plan must detail how a spillage in any of the CSP's data storage facilities of offerings is able to be remediated.

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. Refer to 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*[71]. 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 decommissioned devices by sanitizing them in accordance with NSA/CSS Storage Device Declassification Manual 9-12[72].

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 cyberspace defense and access control services
- Mission system/application protections and integration into required DODIN cyberspace defense and access control services

DoD's usage of commercial cloud services means that the DoD joins an ecosystem of internet-connected CSPs/CSOs. While DoD leverages internet-connected CSOs for the dissemination or processing of public information (Level 2), DoD also leverages private connectivity to the same

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

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

CSOs for the protection of sensitive DoD information i.e., CUI at levels 4 and 5. Additionally, DoD mission partners that are not native to NIPRNet will need to leverage internet-connected CSOs for their level 4/5 processing (possibly under waiver) or will need to implement their own private connectivity.

Figure 5-8: NIPRNet/Commercial/Federal Cloud Ecosystem

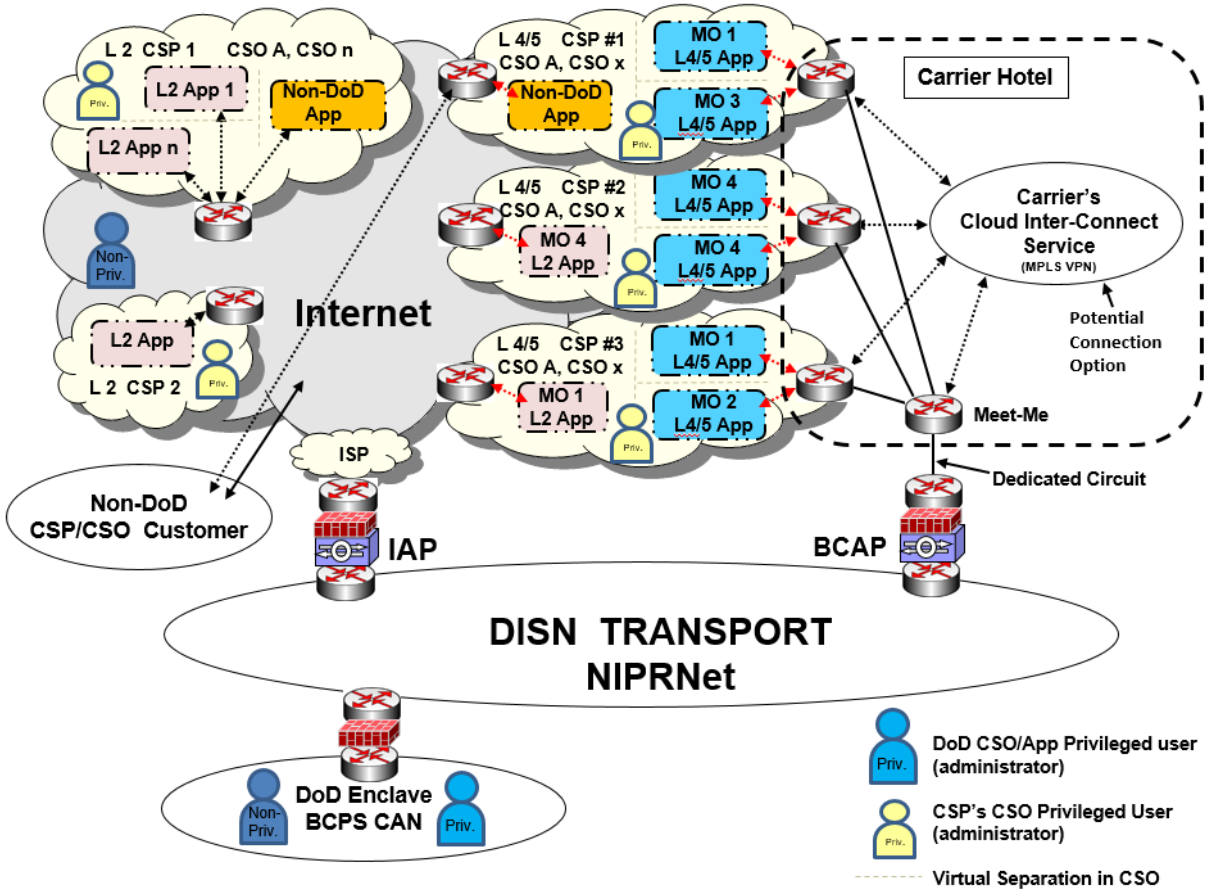


Figure 5-8: NIPRNet/commercial/federal cloud ecosystem shows the overall architecture of the cloud ecosystem into which NIPRNet is connected that consists of off-premises, non-DoD-private commercial and federal CSPs/CSOs. Any of the CSP/CSO clouds in the diagram may be a commercial CSO or a CSO operated/offered by a non-DoD federal agency. The point of this diagram is to make it clear that every non-DoD-private commercial and/or federal CSP/CSO is accessible from the internet even if the CSO has a level 4/5 PA and is connected to NIPRNet via private connections. It also demonstrates that these CSPs/CSOs support non-DoD customers. This figure focuses on NIPRNet connectivity to commercial/federal CSOs for the majority of mission use cases. It does not show all possible situations or use cases. Additional figures may be provided in future releases of the CC SRG.

5.10.1 Cloud Access Point (CAP)

The concept of and requirement for a cloud access point (CAP) is derived from NSA and DoD cybersecurity team guidance as presented in the DoD CIO's *DoD Cloud Way Forward*, v1, 23

July 2014[73] document which provides for a security stack/CAP for both off-premises and on-premises commercially owned and operated CSOs. This concept was made policy by the 15 December 2014 DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services,* which states "commercial cloud services used for sensitive data must be connected to customers through a Cloud Access Point (CAP)." This CC SRG expands upon the concept and adjusts the requirement for on-premises vs off-premises CSOs.

For the purpose of this SRG, sensitive data as referenced in the DoD CIO memo means CUI as handled at levels 4/5 or classified information up to Secret as handled at Level 6.

In general, a CAP is required to mitigate risks to the DISN (or other DoD network[74]) posed by connecting commercial CSOs to it except under certain restrictions. A CAP is a system of network boundary protection and monitoring devices (e.g., firewall, IPS, IDS, proxy, etc.), otherwise known as a cybersecurity or IA stack, through which CSP infrastructure and networks will connect to the network the CAP protects. This CC SRG addresses the DISN as the protected network which includes NIPRNet, SIPRNet, and other DISN-based mission partner/community of interest (COI) networks.

The primary purpose of a CAP is the protection of the DoD network from, and detection of, unauthorized network access from the CSP's infrastructure, CSO management plane, CSP's corporate networks, CSP's connections to the internet, and unauthorized traffic generated from compromised mission owner systems/applications and virtual networks. The secondary purpose is the protection of the DODIN (i.e., DoD information) in general by facilitating protected connections for network users to access level 4/5 or 6 mission owner systems/applications instantiated on IaaS/PaaS, or using SaaS, and the information stored and processed therein, without exposing such traffic to the internet. These purposes also apply to any CAP on any other DoD network, mission partner, or COI network for the protection of those networks and the sensitive information they contain.

NOTICE: a CAP does not protect the cloud-based application or the network enclave (physical or virtual) in which it resides. Each mission owner having control over what is built in the application's virtual environment in I/PaaS, must provide for the protection of their application and virtual network enclave. In the case of CSOs such as P/SaaS where the mission owner does not have control over what is built in the P/IaaS application's environment, the CSP is responsible for the protection of the application and the network enclave (physical or virtual) in which the application resides.

CAP architecture will change depending on whether the CSO infrastructure is on-premises or off-premises and the services transiting it. The concepts of internal CAPs (ICAPs) for on-

[73] DoD Cloud Way Forward: http://iase.disa.mil/Documents/dodciomemo_w-attachment_cloudwayforwardreport-20141106.pdf

[74] For the purpose of this CC SRG, the DISN consists of NIPRNet and SIPRNet. Other DoD networks refer to non-DISN networks such as those operated by certain DoD Components e.g., DREN, Commissary, AAFES, Marines MWR, NDU, etc.

premises CSOs and boundary CAPs (BCAPs) for off-premises CSOs are detailed below with a focus on how these are implemented to protect the DISN. Some CAPs will leverage existing infrastructure and some will be a new capability. CAP architecture may also change depending on the DODIN network, or COI network it is protecting.

The basic capabilities that any CAP must provide in support of DODIN cyber defenses are as follows:

- A firewall capability that will only permit inbound (to DISN) responses to outbound (from DISN) requests to the CSO (all permitted) while denying all traffic originating in the CSO or its management plane except for specifically authorized traffic from the CSO to specific DoD endpoints on the DISN (permit by exception, deny by default). This will address the potential for unauthorized DODIN/DISN access from the CSO management plane or from a compromised CSO.

- An intrusion detection (IDS) capability to detect firewall failure, unauthorized traffic, and malware or other malicious traffic conveyed in unencrypted traffic.

- In the event Voice and/or Video over IP (VVoIP) traffic consisting of the SIP-TLS and SRTP protocols (or their unsecure versions which is not permitted) traverse the CAP, a session border controller (SBC) capability must be implemented. The SBC capability must be implemented in a back-to-back-SIP user agent/proxy mode so a TCP/UDP port is not statically opened inbound signaling. The SBC capability must also dynamically manage the randomly selected ephemeral UDP ports for media (SRTP) such that these IP ports are only opened for the duration of the communications session. Additionally, the SBC capability must act as a SIP/SRTP IDS to detect and report unauthorized activities, malformed/dropped packets, etc.

Note: All of the above capabilities must provide feeds to the DODIN boundary cyber defense capabilities such that anomalies can be detected and correlated with other anomalies on the network and ISs.

The remainder of this section will define the CAP requirements for DISN connected CSOs. These concepts can also be applied to other networks that do not use DISN Transport and are not behind the DISN IAPs.

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

5.10.1.1 Boundary CAP (BCAP) Level 4/5

A Boundary CAP (BCAP) is required to connect off-premises non-DoD (commercially or governmentally) owned and operated CSOs to the DISN (or other DoD networks). A BCAP will interconnect the network it protects with multiple CSP networks that offer private connectivity services. A BCAP does not provide direct internet access to or from CSP CSOs, the mission applications built upon them, or network users.

Refer to Figure 5-9: Notional Connectivity Off-Premises Non-Private Non-DoD CSOs (Commercial/Federal) (NIPRNet IL4/5) at the end of this subsection for a graphic representation of the topics discussed in this subsection and its subsections.

In general, a BCAP will provide the following protections:

- Provides DISN perimeter defenses and cyber defense sensing for traffic to and from applications hosted in the CSO.
- Protects the DODIN (i.e., DoD missions and information 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.

A DISN BCAP is a DISN boundary intended to protect the enclave and information system which is the DISN and its other interconnected enclaves. The DISN is on the inside or protected side of the boundary. Likewise, mission owner systems/applications implemented in I/PaaS or using P/SaaS are considered enclaves which require enclave boundary and demilitarized zone (DMZ) protections (alternate solutions will be considered on a case-by-case basis). These are on the outside or unprotected side of the boundary. As such mission owner systems/applications implemented in I/PaaS as well as P/SaaS applications must protect themselves. This must be accomplished as close to the application enclave boundary as possible. Multiple mission owner systems/applications implemented in IaaS and PaaS where the mission owner has control over the VMs and environment must include virtual enclave boundary and DMZ protections for their application or they can be protected by a Virtual Datacenter Security Stack (VDSS) and managed through a Virtual Datacenter Management Suite (VDMS) as described in the *Secure Cloud Computing Architecture (SCCA) Functional Requirements Document (FRD)*[75]. Mission owner use of PaaS or SaaS where the mission owner does not have control over the VMs and environment, must rely on the enclave boundary and DMZ protections afforded by the CSP for their CSO or leverage an alternative solution (e.g., a third-party CSO such as a cloud access security broker (CASB) service having minimally a FedRAMP moderate PA).

Note: P/SaaS CSOs are typically connected to the internet, thus must have enclave boundary and DMZ protections within their infrastructure to protect their customer's data from internet threats. DoD trusts that this is the case and validates it though the FedRAMP P-ATO and DoD PA processes.

5.10.1.1.1 NIPRNet BCAP

The primary purpose of the NIPRNet BCAP is to protect the NIPRNet from the CSPs/CSOs and to provide private connectivity to the CSP's networks from the NIPRNet in support of NIPRNet user connectivity to IL4/5 Cloud-based applications and services.

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, while the intent is for DISA to

[75] SCCA FRD: http://iase.disa.mil/cloud_security/Pages/index.aspx (PKI required)

implement DISN BCAPs as an enterprise wide DISN service. 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 SCCA FR document.

The NIPRNet BCAP must be implemented as a system of hyper redundant, dual homed, geographically disbursed, high availability, high capacity cybersecurity stacks, and meet-me points so that the BCAP system can handle the throughput required to handle all the applications expected to migrate to commercial Cloud. It provides connectivity between DISN users and multiple off-premises level 4/5 CSOs. It also facilitates user connections to these CSOs from the internet through the DISN IAPs for internet-facing applications (IFAs).

Impact level 2: The NIPRNet BCAP is not used 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. NIPRNet users access these CSOs and applications via the DISN IAPs while internet-based users access them directly. Mission owner applications implemented in I/PaaS CSOs where the mission owner has control over the environment must provide their own enclave boundary and DMZ application protections or leverage an enterprise level application protection service (i.e., the Virtual Datacenter Security Stack (VDSS)/Virtual Datacenter Management Suite (VDMS) portion of the SCCA) instantiated within the same CSO. VDSS/VDMS may be provided by DISA, a DoD component, or the mission owner. SaaS CSOs must provide their own enclave boundary and DMZ application protections to which a mission owner may layer on additional protection services (e.g., CASB). Refer to Sections 5.10.2.2, *User/Data Plane Connectivity* and 5.10.2.3, *Management Plane Connectivity* for additional details. Alternately Level 2 IFAs may be implemented in a Level 4/5 CSO thus will connect either to the internet directly or through the IAPs and NIPRNet BCAP. Refer to *Impact Levels 4/5* below.

Note: All IFAs providing access to publicly released information along with some IFAs providing access to low confidentiality private information should migrate to a Level 2 CSO rather than a level 4 or 5 CSO. This will not only reduce the load and required capacity on the BCAP infrastructure and IAPs but will also reduce the attack surface of the NIPRNet and will permit the DoD components and department to realize the greatest cost savings and support other mandated cost saving initiatives.

Impact levels 4/5: Except as approved (waivered) by DoD CIO, all DoD traffic from NIPRNet (or other DISN-based COI network) 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 IL4/5 traffic is permitted to/from the internet except via the NIPRNet IAPs and DMZ capabilities provided by the mission owner, a DoD component, or DISA. The BCAP or an attached meet-me point provides for direct physical or logical connectivity between the DISN and CSP's network through which the CSO is accessed. Physical connectivity is established using a direct fiber optic connection between the DISN meet-me point router and a nearby CSP network router. Logical connectivity is established using dedicated long-haul circuits, Private IP VPN services, a FedRAMP authorized multi-CSP/customer interconnection service, or a point-to-point IPsec VPN. These connections can also support the transport of IPsec VPNs 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/cybersecurity defense tool

connectivity to internal DISN native cybersecurity defense monitoring systems. Refer to 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 also provide the following functions:

- Serves as an authorized DoD DMZ for IFAs and mission systems in level 4/5 CSOs providing the DISN facing DoD IP addresses used by the mission system/application are authorized DoD DMZ IP addresses. Mission owner applications in I/PaaS must provide their own DMZ application protections or leveraging an enterprise level application protection service (i.e., the Virtual Datacenter Security Stack (VDSS)/Virtual Datacenter Management Suite (VDMS) portion of the SCCA) provided by DISA or a DoD component in the cloud. A BCAP does not support/provide direct internet access to a level 4/5 CSO. Such access must be via the NIPRNet IAPs.

- May terminate physical or logical connections from the internal side of a DoD Component's DMZ such that the DoD component's existing DMZ protections may be leveraged for their IFAs.

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. In this situation, internet-connected users will not be able to use the level 5 service/resource. Mission owners that need this restriction for level 4 CSOs must add the requirement to their SLA/contract.

Note: It is recognized that certain missions that handle CUI (i.e., IL4/5 applications) primarily support internet-based users rather than NIPRNet based users. As such, it might be advantageous for the mission owners of such applications to seek DoD CIO approval (waiver) to host their application and information in a CSO with a DoD IL4/5 PA, but to connect it directly to the internet rather than forcing their internet user traffic through the IAPs and BCAP. If approved, the mission owner must protect their application and information IAW the protection defined above for IL2 applications.

5.10.1.1.2 NIPRNet BCAP Meet-Me Points

A NIPRNet BCAP Meet-Me Point is a DISN point-of-presence (PoP) located in a carrier agnostic commercial network interconnection facility or commercial carrier's collocation facility. This PoP minimally consists of a high capacity router but may include DISN boundary protection capabilities that constitute all or part of the BCAP cybersecurity stack.

The purpose of the BCAP meet-me point is to facilitate the interconnection of the DISN BCAP with multiple CSP networks. Multiple BCAP meet-me points will be implemented to facilitate redundant and reliable interconnection with CSP networks. BCAP meet-ne points will be geographically disbursed in U.S. jurisdiction to facilitate connection availability and to reduce

latency between the users and CSO. The BCAP and/or meet-me points may also support interconnection with commercial carrier grade services that provide cloud customer network access/connection to multiple CSP networks (e.g., Equinix Cloud Exchange, AT&T NetBond, and Verizon Secure Cloud Interconnect). The use of such networks requires that the service be authorized by DoD in advance.

Since the meet-me point is a DISN PoP located in a commercial facility, the following requirements apply. A BCAP meet-me point/DISN PoP located in a commercial facility:

- Must be located in a physically separate protected space within the commercial facility such as in a locked cage or minimally in a locked cabinet.
- The physically separate space is minimally protected as follows:
    - Physical access to the commercial facility is compliant with all required physical environment and maintenance personnel access security controls in the FedRAMP moderate or high baseline (PE and MA families) as appropriate to include but not limited to role-based access control, access auditing, visitor access logging and escorting as needed, etc.
    - Physical access to the DoD space is compliant with all required physical and maintenance personnel access security controls in the FedRAMP moderate baseline or high baseline as appropriate and/or appropriate CNSSI 1253 baselines to include but not limited to role-based access control, access auditing, visitor access logging and escorting as needed, etc.
    - Personnel access to the DoD space is controlled by an automated entry access control system (AECS) that is token and/or biometric based. This system may be under DoD control or under the control of the facility owner, but must limit access to only authorized individuals, must log/audit all accesses to include the identities of the personnel accessing and departing, and must provide and log alerts for unauthorized accesses and failed attempts.
    - Access to the physical space is externally monitored by the facility owner using video cameras and physical intrusion detection system (IDS) alarm systems.
    - It is highly recommended that the internal space be monitored by an automated motion IDS system and video cameras operated by DoD. In this manner DoD can monitor all physical activities within the space, authorized or unauthorized.
- Must be compliant with DoD SRGs and STIGs.
- Must follow a change management and connection approval process that documents all aspects of approved connections and system modification
- All connections are assigned a command communications service designator (CCSD) for tracking and authorization purposes

- Must be assessed and authorized under DoD RMF as part of the BCAP and DISN accreditation due to its role as an extension of the DISN authorization boundary.

5.10.1.1.3 CSP Support for BCAP Connectivity

To support BCAP connections between DoD and an off-premises level 4/5 CSP, the CSP must offer a private connection service to the CSO that does not traverse the internet. The CSP's network must include a PoP in a carrier agnostic commercial network interconnection facility or commercial carrier's collocation facility where an existing DISN PoP/BCAP meet-me-point is located. A physical connection within the facility will be installed between the two PoPs providing a direct private connection between the DISN BCAP and the CSP's network over which the CSO will be accessed along with supporting services. In the event reliability is a requirement for access to the CSO the interconnections must be implemented minimally in two geographically disbursed network interconnection/collocation facilities.

As a condition for a DoD level 4 or level 5 PA the CSP must offer the private connection service for access to the CSO. DoD recognizes that the CSP may not have one or more PoPs collocated with a DISN BCAP meet-me-point. As such the existence of such a CSP network PoP will not be required for obtaining the PA but a willingness to install such a PoP or to negotiate a mutually agreeable location for collocating the DISN and CSP PoPs, or use an approved intermediary cloud interconnection service (having its own DoD PA). Associated costs will be negotiated between the mission owner and CSP. If a new DISN meet-me PoP is required; DISA must be included in such negotiations. Notice of this potential situation must be provided during the PA assessment phase. Such negotiations will occur in the planning stage for the BCAP connection based on a contract between the CSP and their first mission owner. Mission owners may also stipulate that the CSP must have/install a PoP collocated with one or more DISN meet-me-points.

5.10.1.1.4 CSP/CSO Network Connectivity to Internet and BCAP

Section 5.10, Architecture, and Figure 5-8: NIPRNet/Commercial/Federal Cloud Ecosystem, depict the reality that CSPs/CSOs having a level 4/5 PA that are connected to the NIPRNet via a NIPRNet BCAP are also connected to the internet.

As a condition for a DoD level 4 or level 5 PA the CSP, when the CSP's network which supports a DoD contracted CSO is privately connected to the NIPRNet via a NIPRNet BCAP (or other DoD network via their BCAP) and the internet, the CSP must provide evidence that the CSP's network or the CSO cannot provide a path from the internet to the NIPRNet (or other network), thus creating a back door to a DoD network. An additional or associated consideration is the robustness of the CSP's required boundary protection (defense-in-depth security/protective measures) implemented between the internet and the CSO for its protection from internet-based threats. This protection is expected to be different depending on whether the CSO is I/PaaS or P/SaaS and whether the mission owner has control over their portion of the CSO. Refer to Section 5.10.3, CSP Service Architecture, and Section 5.10.6, Mission Owner System/Application Requirements Using IaaS/PaaS, for details.

Figure 5-9: Notional Connectivity: Off-Premises Non-Private Non-DoD CSOs (Commercial/Federal) (NIPRNet IL4/5)

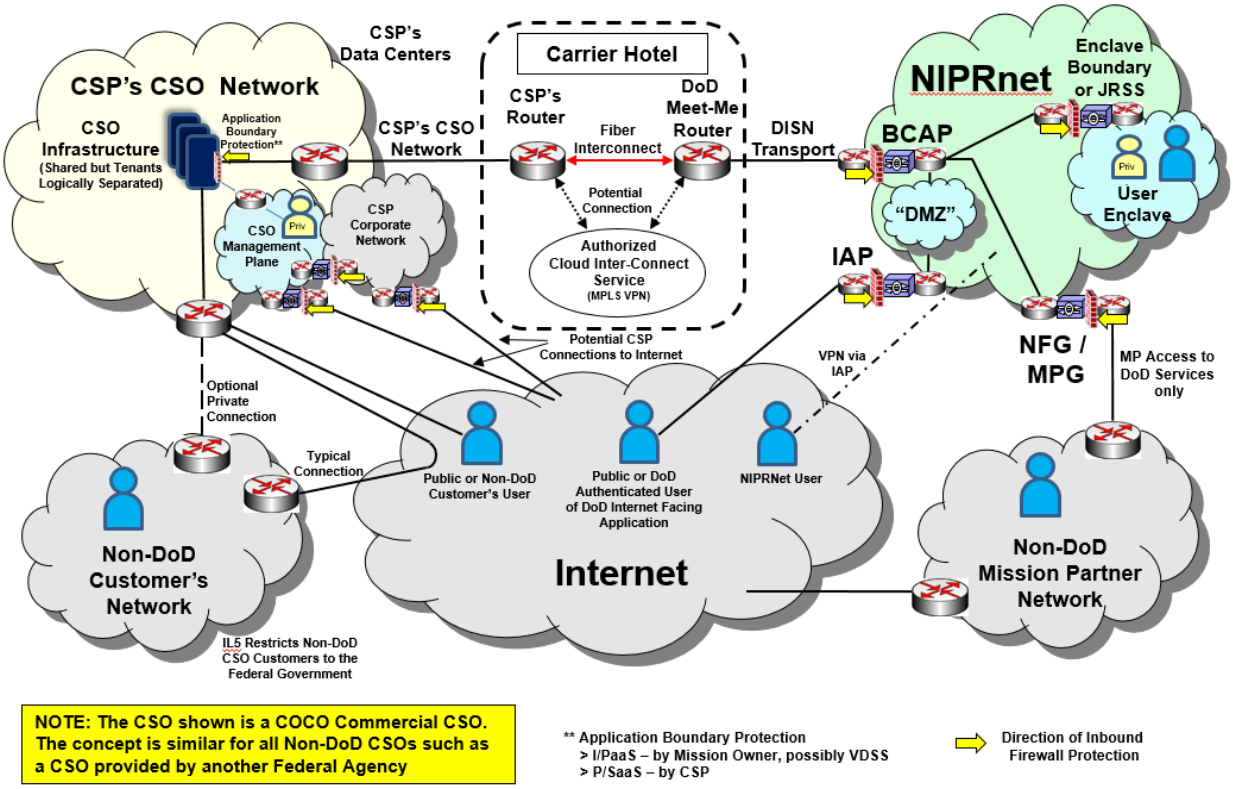


Figure 5-9 notionally depicts the method by which off-premises, non-private, non-DoD CSOs are connected to NIPRNet and other networks as well as how various user communities access the CSO. It supports the topics discussed in Section 5.10.1.1 and its subsections. The following are important takeaways from the diagram:

- The CSP's network through which the CSO is accessed is connected to NIPRNet through the BCAP and meet-me points creating a private connection. This connection is typically a fiber jumper between the meet-me router and the CSP's network router. This connection may optionally be made via an authorized cloud inter-connect service providing access to multiple CSP's CSOs.

- The CSP's CSO will be connected to the internet to support connections from Non-DoD customers of the CSO. These customers may optionally connect via their own private connections. If public users are supported, they will connect via this internet connection.

- The CSP's CSO will be managed from the CSP's management plane which may be connected to the CSP's corporate network, one or both of which will have one or more connections to the internet. Both of these may extend worldwide touching multiple locations/CSO instances and other CSOs.

- NIPRNet users accessing DoD services from the internet including those based in the cloud will VPN into the NIPRNet to access these services.

- Non-DoD and public users accessing DoD IFAs from the internet will do so via the IAPs (and DoD DMZ as applicable). This includes authenticated users of DoD IFAs. Direct internet access is only permitted under DoD CIO approval (CAP waiver).

- Non-DoD mission partner networks accessing DoD services, whether cloud based or not, access the NIPRNet via the NIPRNet federal/mission partner gateway(s). Access to the CSO for their own use will be the same as the non-DoD customer's network.

5.10.1.2 Internal CAP (ICAP)

Impact levels 2/4/5: Internal CAPs (ICAPs) will be implemented for on-premises commercially owned and operated CSO connectivity to the DISN, if the CSO management plane has connectivity to external networks that bypasses native NIPRNet enclave and external boundary (IAP) protections. As such all NIPRNet (or other unclassified COI network) production traffic to and from on-premises commercially owned and operated CSP infrastructure serving Level 2, 4 and 5 missions and the mission virtual networks must traverse an ICAP.

An ICAP is a DISN boundary consisting of a cybersecurity stack that protects the DISN (or other DoD network) or the datacenter network to which the CSO is connected (inside/protected side of the boundary) from, and provides detection of, unauthorized network access from the CSP's infrastructure (outside/unprotected side of the boundary), externally connected CSO management plane, CSP corporate networks, CSP connections to the internet, and from compromised mission owner systems/applications and virtual networks. Typically, one ICAP is required for each physical CSO infrastructure instance.

An ICAP is required to mitigate vulnerabilities and risks associated with implementing a commercial CSP's CSO infrastructure on-premises (i.e., located inside the B/C/P/S physical or virtual "fence-line.") when, as expected, that infrastructure is managed by the CSP from their off-premises corporate CSO management centers using non-DoD controlled workstations and infrastructure which will most likely have some connectivity to the CSP's corporate network and/or the internet. The connection between the CSO management centers and the on-premises CSO's management plane is expected to traverse an IPsec tunnel across NIPRNet, its IAPs, and internet OR traverse a dedicated "side-door" connection using a dedicated circuit, a commercial carrier's Private IP VPN service, or restricted internet service provider (ISP) connection. ISP connections, across which the CSP must VPN, must not provide inbound or outbound access to/from CSO management plane to/from the open internet. This requirement also applies if the CSO management plane is locally dedicated to the CSO and managed on-premises, but with an external connection to the CSP's corporate network, or similar.

The ICAP will be configured to pass authorized production traffic (i.e., required protocols and services on their approved IP Ports) for those mission applications using the CSO while blocking all access to DISN or the datacenter network to which the CSO is connected from the CSO management plane.

The architecture of ICAPs may vary and will be developed based upon the location of the CSO infrastructure on the BCPS, existing infrastructure, and other factors. An ICAP minimally consists of a firewall and IDS functions but may leverage current capabilities in the cybersecurity stack, Joint Regional Security Stack (JRSS), or future technology such as JIE core data center.

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, the full suite of BCAP boundary protections are not needed.

When using the cybersecurity stack protecting a DoD data center today (e.g., DECC) or JIE core data center in the future as an ICAP, the CSO must be connected in such a manner that both the DISN and datacenter network are protected from the CSO management plane.

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.

An ICAP is not required in the event the CSO is managed under the following conditions:

- The CSO management plane is a closed network directly part of the CSO infrastructure having no side-door or back-door connections to non-DISN networks.

OR

- The CSO management plane is a NIPRNet enclave or part of one which only has connectivity to external networks such as the internet or CSP corporate network via, and visible to, the native NIPRNet boundary protections and IAPs. While CSP personnel may VPN to their corporate network from their workstation, a point-to-point VPN may not be established between the CSP's network and the CSO management plane. The latter will require the establishment of an ICAP.

Additionally:

- CSP personnel manage the CSO from a location on a DoD installation/BCPS.
- The CSP personnel are issued GFE from which they perform their CSO management duties if these workstations can access the NIPRNet.
- CSP personnel may not use the same GFE to manage the CSO as is used to perform general business functions such as email or those that might require surfing the internet.
- The CSP personnel are issued CAC cards for installation/BCPS access and access to their GFE and NIPRNet.

Figure 5-10: Notional Connectivity: On-Premises DoD Private CSOs & OFF-Premises Management Requiring ICAP (NIPRNet IL4/5)

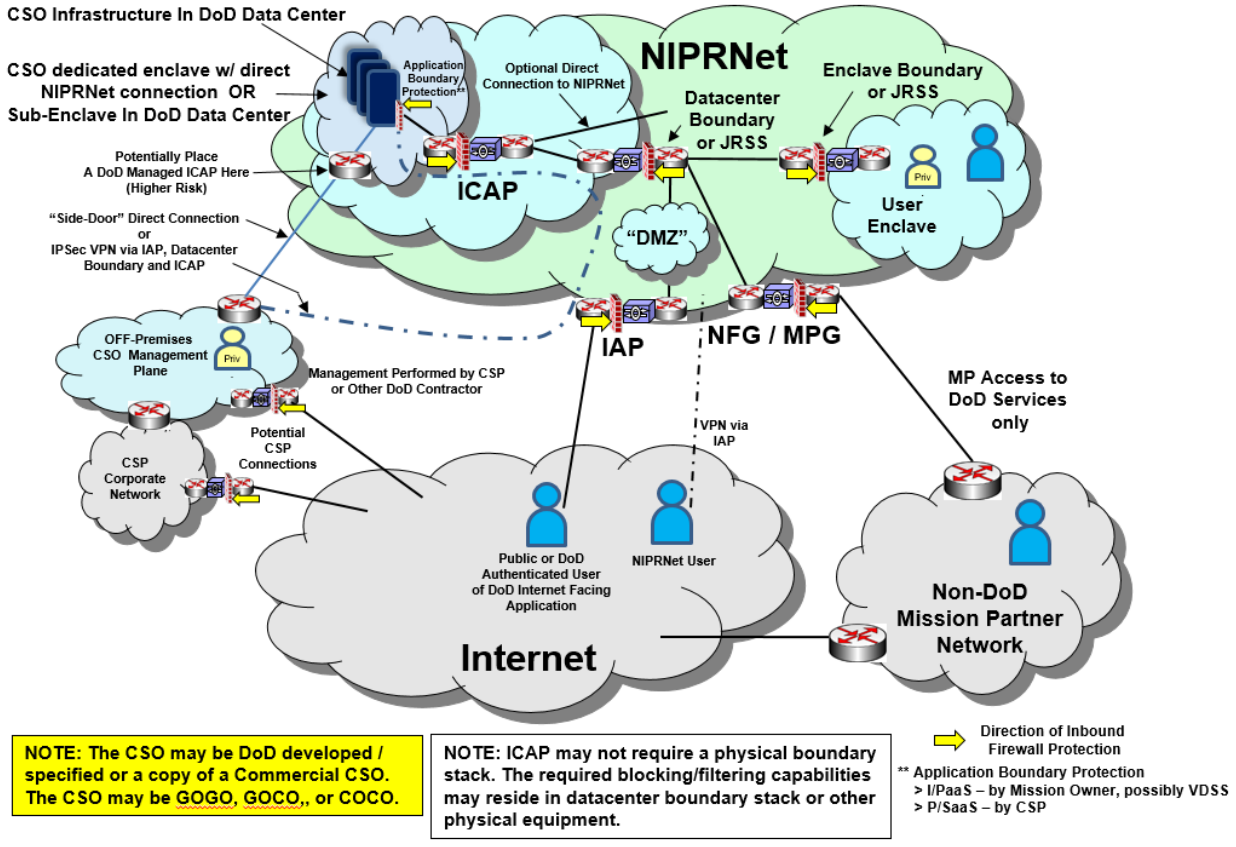


Figure 5-10 notionally depicts the method by which on-premises DoD private CSO infrastructure is connected to NIPRNet when the CSO is managed from a contractor's off-premises management plane. This may apply to COCO or GOCO CSO infrastructures. It supports the topics discussed in Section 5.10.1.2. The following are important takeaways from the diagram:

- If the on-premises (private) CSO infrastructure is managed from an off-premises non-NIPRNet CSO management plane or contractor enclave an ICAP is required. This is due to the likely connection to a corporate network, both of which may have one or more connections to the internet.
- Connection from the off-premises CSO management plane to the CSO infrastructure may be via an encrypted tunnel that traverses the IAP, NIPRNet, data center boundary (if inline), and the ICAP, OR via a direct "side door" connection (i, e., direct circuit or dedicated ISP connection).
- NIPRNet users accessing DoD services from the internet including those based in the cloud will VPN into the NIPRNet to access these services.
- Non-DoD and public users accessing DoD IFAs from the internet will do so via the IAPs (and DoD DMZ as applicable). This includes authenticated users of DoD IFAs.
- Non-DoD mission partner networks accessing DoD services, whether cloud based or not, access the NIPRNet via the NIPRNet Federal/Mission Partner gateway(s). Access to the CSO for their own use will be the same as the Non-DoD customer's network.

Figure 5-11: Notional Connectivity: On-Premises DoD Private CSOs & On-Premises Management (NIPRNet IL4/5)

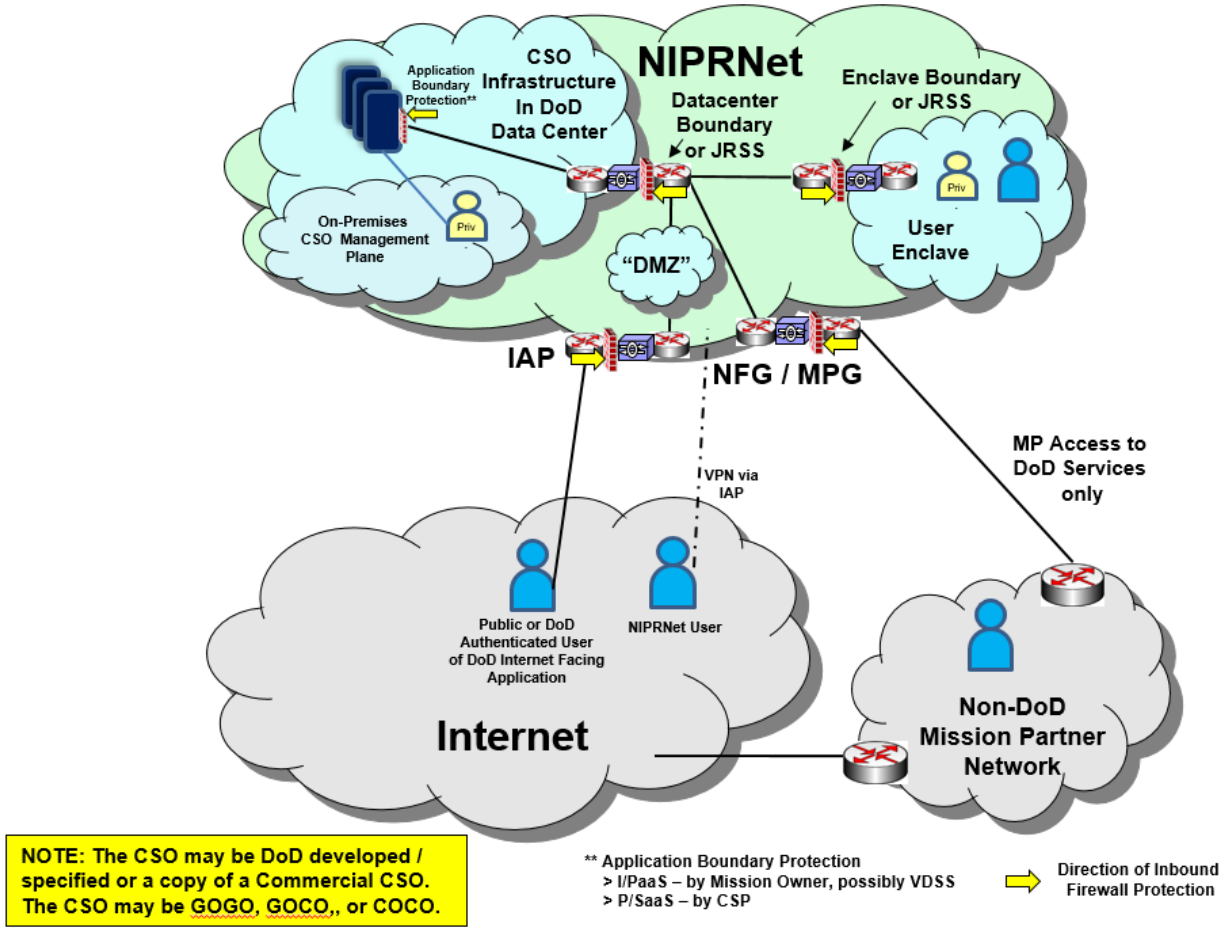


Figure 5-11 notionally depicts the method by which on-premises DoD private CSO infrastructure is connected to NIPRNet when the CSO is managed from an on-premises management plane. This is in contrast to being managed from an off-premises management plane. The following are important takeaways from the diagram:

- ICAP is not needed if CSO management is performed from an on-premises NIPRNet enclave.
- (Not depicted) In the event the CSO infrastructure is directly connected to the NIPRNet, a datacenter enclave boundary must be provided.

5.10.1.3 Virtually On-Premises Architecture NIPRNet Level 4/5

The virtually on-premises concept is discussed above in Section 5.2.1.1, DoD Off-Premises vs. On-Premises vs. Virtually On-Premises. Figure 5-12 provides the graphical depiction of the architecture.

Figure 5-12: Notional Connectivity: Virtually On-Premises DoD Private CSOs & Management (NIPRNet IL4/5)

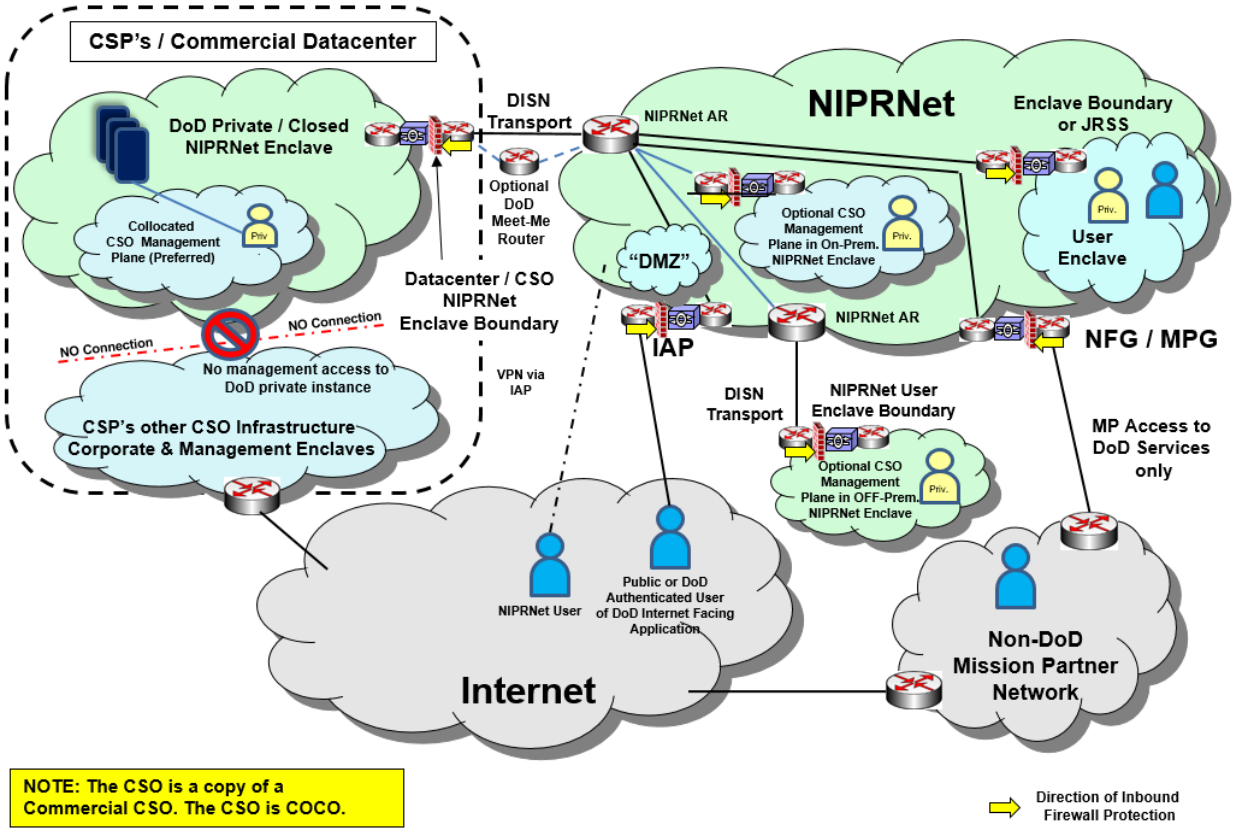


Figure 5-12 notionally depicts the method by which a virtually on-premises architecture can be achieved. The following are important takeaways from the diagram:

- The CSO infrastructure is DoD private in a closed NIPRNet enclave that is off-premises.
- DISN transport is extended to this enclave optionally via a meet-me point. The use of a meet-me point may invoke additional traffic separation requirements depending on the specific off-premises location in relation to the meet-me location and if the hosting parties' network is used.
- The CSO network enclave is protected with DoD NIPRNet datacenter enclave protections or equivalent to include enclave firewall and ID/PS.
- The DoD private CSO infrastructure is managed from the same or another properly protected NIPRNet enclave.
- No management of the private CSO infrastructure may be performed from the CSP's management plane used for any other CSO offered. No such connection is permitted in this scenario. Any connection between the private CSO infrastructure and a non-

dedicated management plane enclave negates the virtually on-premises construct and requires the connection to the NIPRNet to traverse a BCAP.

5.10.1.4 SIPRNet ICAP

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).

Since DoD on/off-premises impact level 6 CSOs and their supporting infrastructure, to include management network(s) are required to be one or more closed SIPRNet enclaves, they can be considered to be on-premises (physically or virtually) for the purposes of this CC SRG due to the concept of extending the virtual "fence-line" or SIPRNet boundary around such DoD enclaves. As such these enclaves must comply with all SIPRNet connection approval requirements which include the appropriate enclave boundary protections and cyberspace defense 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

ICAPS are required as they are for NIPRNet connections to CSOs.

The following diagrams depict the SIPRNet architectures for connecting CSOs and their management enclaves to SIPRNet.

Figure 5-13: Notional Connectivity: On-Premises DoD Private CSOs & On/Off -Premises Management (SIPRNet IL6)

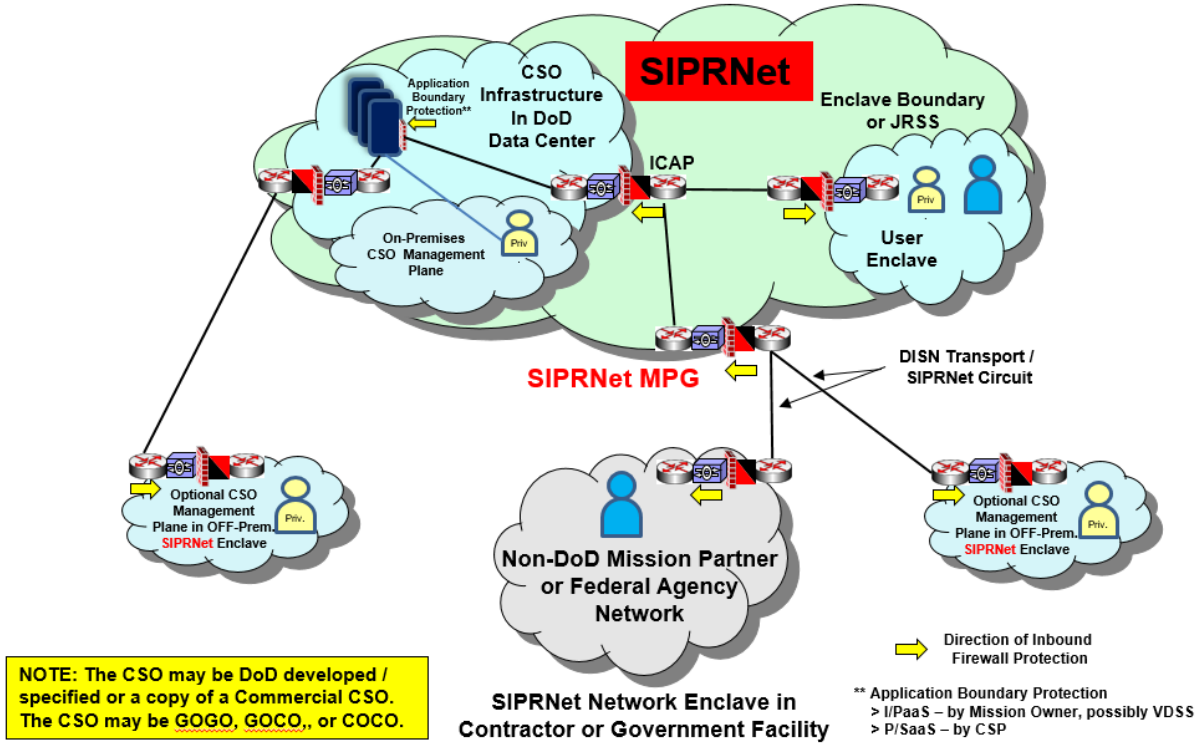


Figure 5-13 notionally depicts the method by which an on-premises IL6 CSO would be connected to SIPRNet. The following are important takeaways from the diagram:

- The management plane is also on SIPRNet within the same or another SIPRNet enclave.
- ICAP is required.
- Non-DoD mission partners or other federal agencies will access the CSO via the SIPRNet mission partner gateway.
- In the event the CSO is managed from a SIPRNet enclave not collocated with the CSO infrastructure, connections to the CSO will be via the SIPRNet mission partner gateway or the CSP may institute a private connection using black transport.

5.10.1.5 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 to include BCAPs and ICAPs depending on the classification level of the network.

Mission partner environments (MPEs) include mission partners that use networks other than NIPRNet or SIPRNet (e.g., DREN) and mission partner communities of interest (COI) that use 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; morale, welfare and recreation (MWR) organizations; non-appropriated fund (NAF) organizations; educational entities (e.g., National Defense University (NDU)) typically operate networks that may not be part of the DISN (i.e., do not use DISN transport or NIPRNet services such as internet access via the NIPRNet IAPs) or .mil domain. These mission partners and their networks may be 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 and authorize 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.

While the CAP concepts presented here are applicable to non-native DISN networks operated by other DoD components (e.g., the .edu community which supports a diverse non-DoD user base) there may be other methods of protecting these networks from risks associated with the use of commercial cloud. The use of a cloud access security broker (CASB) service having minimally a FedRAMP moderate PA might be one such alternative for non-DISN networks.

MPEs that use 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

SCCA Functional Requirements Document (FRD)[76] when connecting CSP infrastructure to their networks. MPEs implemented as a COI overlay on NIPRNet or SIPRNet can use the DISA-provided CAPs to fulfill the CAP requirement or may provide their own CAP capability IAW the SCCA. 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.

Note: MPE network connectivity/access to off-premises commercial DoD level 4/5 CSOs will not traverse a NIPRNet BCAP or a NIPRNet federated gateway (NFG) when connecting to/accessing MPE applications instantiated in such a CSO.

5.10.1.6 Mission Partner Environment Access to NIPRNet Services Hosted in the Cloud

Mission partner environments that require access to NIPRNet services are required to connect to NIPRNet via the internet, IAPs, and DoD DMZ or via a NIPRNet federated gateway (NFG) IAW JFHQ-DODIN TASKORD 16-0103 Establishment of the NIPRNET federated gateway (NFG). NIPRNet services are applications operated by DoD components for the purpose of serving NIPRNet users. Some of these NIPRNet focused applications might be implemented in a CSO. Such a CSO might be commercial off-premises CSO, a DoD private off-premises CSO, or a DoD private on-premises CSO. Mission partners that desire or require access to such applications must coordinate with the mission owner of the application for permission to access it and to determine the best access method. There are three approved methods of accessing such an application as follows:

- The MPE user must establish a VPN connection to NIPRNet or the application itself.
- The mission owner must expose the application to the internet through the DoD DMZ such that the MPE user can access the application from the internet via the IAPs.
- The mission owner must expose the application to the MPE network and MPE users through the NFG.

5.10.1.7 Mission System Connection Approval through DISN BCAPs

Impact levels 4/5: 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. Specific processes and procedures regarding connection approval and mission owner connections

[76] SCCA FRD: Link to be added when published

[77] SNAP: https://snap.dod.mil/gcap/home.do

Connection Approval: http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Approval

via a BCAP are addressed in the DISA Cloud Connection Process Guide (CCPG)[78] which will ultimately be merged with the overall DISN Connection Process Guide (CPG)[79].

Impact level 6: 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 CPG. Approval for connection to the SIPRNet will be processed through the DISA classified connection approval process like any other SIPRNet enclave.

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 5-4 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 5-4: 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	▪ 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

[78] CCPG: http://disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/CCPG.pdf

[79] CPG: http://disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/DISN_CPG.pdf

Impact Level	Off-Premises Non-DoD CSP Service Offering Infrastructure	On-Premises DoD and Non-DoD CSP Service Offering Infrastructure
	connecting from inside the DISN (i.e., NIPRNet) will connect to the internet via the DISN IAPs and then to the CSP infrastructure. ▪ CSO connections will be assessed and authorized using the same external connection requirements as any other internet-facing connection.	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 IAPs and then an ICAP. ▪ CSO connections will be assessed and authorized the same as any other internal connection.
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. 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.	
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).	▪ 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

Impact Level	Off-Premises Non-DoD CSP Service Offering Infrastructure	On-Premises DoD and Non-DoD CSP Service Offering Infrastructure
	▪ 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)[80] Suite B). ▪ 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.	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.

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 5-5 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 or FIPS 140-3 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

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

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 5-5: 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 IAPs. ▪ **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 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 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.
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	▪ **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-

Impact Level	Mission Owner Management Plane	CSP Management Plane
	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.	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 use existing infrastructure such as the Enterprise Services Directorate (ESD) Out of Band (OOB) management network. No service provider security stack is required.
Level 6	▪ All management and monitoring connectivity is via the SIPRNet. Management and monitoring traffic will be encrypted using FIPS 140-2 or FIPS 140-3 validated cryptography[81] to accommodate separation for Need-to know reasons.	▪ **DoD CSP on-premises service offering infrastructure and management:** CSP management connectivity will use 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

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

Impact Level	Mission Owner Management Plane	CSP Management Plane
		infrastructure if personnel are collocated using their SECRET LAN. An encrypted, tunneled connection using FIPS 140-2 or FIPS 140-3 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 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 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.

Due to the normal internet connectivity for CSOs, DoD expects defense-in-depth security/protective measures to be established by the CSP for P/SaaS CSOs where the mission owner does not have control of their infrastructure environment. These are, but are not limited to, the following:

- Application Layer and Web application Firewall(s) (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 tiered architecture which provides "front end" 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. 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.

  Note: P/SaaS CSOs in which the mission owner does not have control of their infrastructure environment typically serve NIPRNet users, thus are NIPRNet-facing via the BCAP. It is recognized that some mission owners need a portion of their CSO application to be internet-facing. In such cases, the internet/NIPRNet-facing portion of the application must use a separate web server(s) and IP address(es) from those only facing the NIPRNet such that they can be whitelisted for access via the IAPs for access and protect the NIPRNet facing web server(s). Refer to Sections *5.10.4.1 IP Addressing*

of CSOs and Mission Owner Systems/Applications and *5.17.2 DoD DMZ Whitelist* for additional information.

Note: The internet-facing IP addresses will also be available for access from the NIPRNet.

- Customer data-at-rest encryption protections using FIPS 140-2 or FIPS 140-3 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 or FIPS 140-3 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.

Notes:

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

- 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 or FIPS 140-3 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[82] 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 website 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 Network Information Center (NIC) Registry Protocol 9802 then goes on to state that:

> "a. ... IP address space is assigned by the DoD NIC[83] 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 only to be used on DoD systems located on or connected to as an extension of the NIPRNET or SIPRNET.

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.

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

[83] DoD NIC Website: https://www.nic.mil/

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. RFC 1918 addresses are "private" (non-publicly routable) which are permitted/used within DoD network enclaves and within CSO enclaves behind the external publicly routable addresses.

5.10.4.1 IP Addressing of CSOs and Mission Owner Systems/Applications

Off-Premises Impact Level 2 IaaS/PaaS/SaaS:

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 where the mission owner has control over their IP addressing 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 for a .mil URL to point to the commercial URL and its IP address. Similarly, PaaS or SaaS CSOs where the mission owner does not have control over the IP addressing will be addressed using public IP addresses assigned and managed by the CSP.

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 NIC[84] 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 and PaaS 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

[84] DoD NIC Website: https://www.nic.mil/

aside a range of NIPRNet IP addresses for CSOs connected to the NIPRNet BCAP. Mission owners/CSO sponsors may make IP address requests through the DoD NIC Website[85].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 BCAP is acceptable.

DoD's objective requirement for all off-premises Level 4/5 CSP's PaaS and SaaS CSOs serving the DoD where the mission owner does not have control over IP addressing, 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 and accessed via the private connection and BCAP. In this case, customer-facing interfaces include general user interfaces and customer management interfaces including CSO customer service management/ordering portals. DoD does not want to be required to access such portals via the internet except during initial setup of the CSO.

This IP addressing requirement does not include CSP systems instantiated within the CSO infrastructure that are not customer facing or directly accessible from the NIPRNet (or other mission partner network). Such internal systems and infrastructure may use CSP assigned and managed IP addresses.

In the event a mission owner's application in I/PaaS where they have control of the addressing, or the P/SaaS CSO where the Mission Owner does not have control of the addressing, must face both NIPRNet and internet via the BCAP, separate IP ranges must be assigned to the NIPRNet-only facing servers from those assigned to servers available from NIPRNet and the internet. This is to facilitate registering the internet-facing IP addresses as DoD DMZ addresses and adding them to the DoD DMZ/IAP whitelist while protecting the NIPRNet facing servers from internet threats.

Level 4/5 Commercial IP Addressing and Routing for SaaS and Some PaaS:

DoD recognizes that with some off-premises commercial SaaS and PaaS CSOs today, it is not possible or practical for the CSO to support customer IP addressing for several reasons. In such cases, the Mission Owner will not have control over the IP addressing of the CSO as would be the case with a "bring your own" IP address capability and therefore, CSP managed commercial IP addresses must be used and interfaced with the NIPRNet via the BCAP. DoD's preferred solution is for the CSP to provide a NAT or proxy between the CSO and NIPRNet BCAP so that NIPRNet need only route DoD IP addresses.

Alternate solutions that require a CSO's commercial IP addresses to be routed on the NIPRNet must be assessed and approved through a Non-DoD addressing risk assessment and risk acceptance process which may affect the ability of the CSO to be awarded a DoD PA or may

[85] DoD NIC Website: https://www.nic.mil/

result in a PA with conditions. The CSP must work and coordinate with DISA to achieve such an alternate solution to minimize the operational and cybersecurity effects on the DISN/NIPRNet.

The following is a set of minimum constraints and requirements that will be considered for the Non-DoD addressing risk acceptance/PA conditions and must be adhered to for ongoing operations:

- Vendors shall provide a complete list of their commercial IP subnets that need to be routed on NIPRNet in order to affect such routing.
    - These route advertisements must be aggregated to /24 or larger blocks in support of current DISN capabilities. Although changes are to be expected over time, the frequency of changes to the list must be minimal to lessen the management burden on DISA Operators, and to reduce network service disruptions.
- Commercial IP subnets advertised to NIPRNet via the BCAP used to access DoD services and applications in off-premises CSOs must be dedicated to DoD and separate from the IP addresses used to access the CSO from the internet.
- Commercial IP subnets advertised to NIPRNet via the BCAP used to access DoD services and applications in off-premises CSOs must not also be advertised to the internet from the CSP's infrastructure, or if so, they must not be reachable from the internet (i.e., L4/5 DoD accounts, services, and applications which, per DoD policy, are only to be accessible from the NIPRNet must not be accessible directly from the internet). This means that the same IP addresses must not be used for accessing the CSO from the NIPRNet that are used for accessing it from the internet. This will cause routing issues for both parties.
- In the event a mission owner's application in P/SaaS CSO where the mission owner does not have control of the addressing must face both NIPRNet and internet via the BCAP, separate IP ranges must be assigned to the NIPRNet-only facing servers from those assigned to servers available from NIPRNet and the internet. This is to facilitate registering the internet-facing IP addresses as DoD DMZ addresses and adding them to the DoD DMZ/IAP whitelist while protecting the NIPRNet facing servers from internet threats.
- While DoD expects the CSO's commercial IP addresses used to access L4/5 DoD accounts, services, and applications in the CSO via the BCAP and private connection to be dedicated for DoD NIPRNet user access, in the event the CSO must use the same IP addresses for access by all CSP/CSO customers, whether DoD or non-DoD, (this assumes the non-DoD customers access is via the internet) then the CSP must take extra precautions to prevent the CSO's internet connection or a compromised system from becoming a back door to the NIPRNet. Furthermore, the CSP must also ensure that direct traffic to the CSO from the internet is not potentially routed over NIPRNet.
- DISA will NOT advertise any CSP's commercial IP subnets used for both direct internet access and NIPRNet to the internet via the NIPRNet IAPs. Doing so could cause unauthorized traffic to the CSO from the internet to attempt to traverse the NIPRNet.

DISA cannot support such traffic for both operational and cybersecurity reasons. Only DoD IP addresses associated with .mil URLs or a CSO's DoD dedicated commercial IP addresses accepted as routable on NIPRNet may be advertised to the internet via the IAPs.

- In the event a mission owner implements a "Cloud" VPN between the BCAP and their Intranet gateway/boundary for a CSO that is also used by other mission owners, the same commercial IP addresses may be visible and reachable from the NIPRNet, internet, and Mission owner's intranet. In this case, it is the responsibility of the mission owner to control their own routing policies. The mission owner shall implement routing and security policies within their network to enforce service access control, during both normal and failure scenarios.

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 network 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 use DoD assigned and managed SIPRNet IP addresses throughout. Alternate internal 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 use 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 use 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 and Some PaaS (All Levels)

While protecting/securing/defending the P/SaaS architecture where the mission owner does not have control of the environment is the responsibility of the CSP, mission owners contracting for and using CSP's P/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. Refer to Section 5.15, *Ports, Protocols, Services, Management and Cloud* for additional information.

- Register the service/application with the DoD DMZ Whitelist for both inbound and outbound traffic if traffic will cross the IAPs. Refer to Section 5.17.2 *DoD DMZ Whitelist* for more information.

Register the Cloud IT Project (CITP) and CSP's CSO in the DISA SNAP database for the connection approval which also includes the designation of a certified CSSP for the performance of mission cyberspace defense (MCD) actions as defined in Section 6, *Cyberspace 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 CSSP community is aware and informed of the CITP such that they can perform their cyberspace defense duties described in . Section 6, *Cyberspace Defense and Incident Response.*

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

5.10.6 Mission Owner System/Application Requirements Using IaaS/PaaS

This section provides mission owners with an overview of the items they need to address when using an I/PaaS CSO where they have control of over the environment. This is partly to alleviate the perception that putting an application in the cloud takes care of all security responsibilities. The items here reflect general DoD policy.

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 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/private DMZ zones with appropriate protections for

internet/NIPRNet-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 DMZ protections in addition to a zoned architecture described above . For example, this may include the following (adapted for cloud):

  - Web server in a public virtual network zone (unrestricted or restricted)
  - Application and database servers in one or more private virtual network zones
  - 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 CSSP 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 and 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 CSSP responsible for the mission system/application. Refer to Section 6, *Cyberspace Defense and Incident Response* for more specific information.

- IaaS: Securely configure (harden/STIG)/patch/maintain each VM's OS and IAW DoD policy and U.S. Cyber Command direction (USCYBERCOM). 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 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.

- IaaS/PaaS: Configure virtual networks such that CSO API calls remain on the CSP's network, not having to traverse the CAP/NIPRNet and internet. This may require a second gateway from the virtual network to the CSP's network that is restricted to the IP addresses of the API servers.

- 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. Refer to 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 or FIPS 140-3 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.
    - Use an HBSS agent control server (EPO) within NIPRNet or an associated common virtual services environment in the same CSO (e.g., VDMS).
    - Implement a secure (encrypted) connection or path between the HBSS agents and their control server.
    - Provide visibility by the Mission Owner's CSSP entities as defined in Section 6, *Cyberspace Defense and Incident Response*.

- Implement scanning using an Assured Compliance Assessment Solution (ACAS) server IAW USCYBERCOM TASKORD 13-670.

    - Use an ACAS Security Center server within NIPRNet or within an associated common virtual services environment in the same CSO (e.g., VDMS).

  - Implement a secure (encrypted) connection or path between the ACAS server and its assigned ACAS Security Center.

- Provide visibility by the mission owner's CSSP entities as defined in Section 6, *Cyberspace 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 or FIPS 140-3 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. Refer to 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. Refer to 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. Refer to Section 5.17.2 *DoD DMZ Whitelist* for more information.

- 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 CSSP to perform MCD Actions. 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 CSSP community is aware and informed such that they can perform their Cyberspace Defense duties described in Section 6, *Cyberspace Defense and Incident Response.*

- Implement Cyberspace 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. Active Directory Integration for Cloud

Active Directory (AD) implementations (if needed) will be configured IAW the Active Directory Domain and Forest STIGs[86] 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)

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

- 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.

5.10.6.1 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.

5.10.6.2 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"[87]. 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.

5.10.7 Hybrid Cloud-Interconnections Between CSOs

There are several reasons why various IL4/5 or IL6 CSOs need to be interconnected. The following sections will address some of the security and architectural constraints surrounding each.

Note: In the event of the interconnection of a higher impact level CSO with a lower impact level CSO, the transfer of the higher impact information to the lower impact level CSO must be prevented unless an approved cross domain solution (CDS) is used and appropriate approval procedures are followed.

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

5.10.7.1 Mission Owners Applications

Mission owner's applications or cloud use cases might need to leverage multiple off-premises CSOs for various reasons. For IL4/5 or IL6 CSOs, the interconnection of these CSOs must be monitored such that unauthorized traffic and information transfer is avoided and audited.

- Connections between CSOs from the same CSP will remain on the CSP's network.
- Connections between CSOs from different CSPs will traverse the CSO's connections to the meet-me router(s). While not desirable due to circuit capacity usage concerns, some traffic might be routed through the BCAP if deemed necessary.

In all cases, auditing of traffic will be performed by the interconnected CSOs. Some auditing may occur at the meet-me router (or BCAP) for those connections that traverse these points.

5.10.7.2 On/Off-Premises Scenarios

Mission owner's applications or cloud use cases might need to leverage multiple IL4/5 or IL6 CSOs that are both on-premises and off-premises. The interconnection of these CSOs will be via the BCAP.

5.10.7.3 SaaS CSOs Using "External Services"

A commercial CSP, to provide a complete SaaS CSO, may leverage one or more third-party "external services". These may include notification services or scanning and audit services, and/or others. CSOs seeking an IL4/5 PA must ensure that sensitive DoD data is not transmitted to, or via, such external services unless that service has a DoD PA or is addressed in the CSO's PA. If the CSO is an IL4/5 CSO, traffic to and from such services will not traverse the DISN BCAP assuming the CSO serves non-DoD customers. The CSP must ensure that such external service connections, likely to be via the internet, do not permit access to NIPRNet via the BCAP from such connections.

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 use encryption hardware/software on the DISN or a cloud encryption service that provides DoD control of keys and key management. Some CSOs may offer a KMS service that can suffice for management of customer keys by the customer while preventing CSP access to the keys. It is recommended that such CSP KMS services be evaluated by NSA.

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 websites 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 through 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.
    - Refer to 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)
- Using FIPS 140-2 or FIPS 140-3 validated cryptography modules[88] (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
    - OR Order a CSP KMS service that has been evaluated by NSA.

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

[88] NIST FIPS CMVP: http://csrc.nist.gov/groups/STM/index.html http://csrc.nist.gov/groups/STM/cmvp/index.html

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[89]:

"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 databases. 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.

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

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

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 used. 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 fulfillment 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 may be 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 COI 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. Such connections will be appropriately secured for the protection of the organization's network and information/applications in the cloud. The organization's network boundary with the CSP's network will be considered a BCAP and will provide boundary protections and monitoring as required for the protection of the specific organization's network and information it contains. 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 (i.e., contractor owned/operated IT systems used by the contractor to support contractor functions that store DoD CUI) IAW DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*[90] and NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*[91]which primarily focuses on confidentiality.

Non-CSP DoD contractors and DIB partners may wish to use cloud services in the fulfillment of their contract or for the protection/processing of DoD data they possess (i.e., CUI or Covered Defense Information (CDI)). Thus, for the protection of sensitive CUI/CDI, it is highly recommended that Non-CSP DoD contractors use CSOs that have been granted a DoD Level 4 PA. 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 and the protection of information placed in the cloud.

Non-CSP DoD contractors and DIB partners may NOT use CSOs that have been granted a DoD Level 5 PA as such contractors are outside the supported community of Federal agencies until such time as DoD changes this level 5 limitation.

[90] DoDI 8582.01: http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf

[91] NIST SP 800-171: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Note: Non-CSP DoD Contractors and DIB Partners are required to comply with NIST SP 800-171 for the protection of CUI/CDI. The DoD level 4 and level 5 baselines cover all of the C/CE referenced in the SP 800-171 except CM-3(2), CM-7(4), and IR-2(1).

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 use 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 DoD Mission Owner Test and Development in the Cloud

Cloud environments are a good place for mission owners to do application development and testing as well as research testing. Furthermore, test and development activities associated with application lifecycle management for cloud-based applications are best performed in the same cloud environment as the production application. This section addresses DoD test and development (T&D) activities in IaaS and PaaS CSOs where the mission owner has control of the environment.

Note: This section does not directly apply to third-party DoD contractor companies developing applications for DoD in I/PaaS CSOs. Unless stated otherwise in the contract, the contractor may perform their contract activities in whatever environment they choose, in the cloud or not. Therefore, the contractor is responsible for the security of their T&D environment and the security (i.e., CIS) of the code being developed. However, the contractor must follow industry best practice and/or follow the guidance provided here.

Security requirements for DoD T&D and laboratory environments are defined in the suite of Enclave T&D STIGs[92]. Refer to these STIGs on Cyber Exchange for the latest guidance. This section of the CC SRG does not change the security requirements associated for each zone but it adds nuance when operating in the cloud. All T&D Zones instantiated in the cloud must comply with these STIGs except for the nuanced remote access guidance added here.

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.

  Note: Zone A supports or is representative of the environments in which the Director, Operational Test and Evaluation (DOT&E) and Joint Interoperability Test Command (JITC) performs DoD's Test and Evaluation (T&E) on DoD applications and systems.

- 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.

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

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 and should 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.

Application lifecycle management typically involves an application development Zone B, an application test Zone A, and a production zone. Each zone has its own cyber security requirements that must be implemented to protect the zone itself and the DODIN. As with DoD production applications, T&D zones A and B may be instantiated in DoD private I/PaaS CSOs connected to the NIPRNet. T&D zones A and B must also be protected and monitored by the same CSSP as the production zone when implemented in the same CSO.

DoD application test Zone A instantiated in cloud infrastructure must be implemented in the same CSP/CSO with the same information impact level and having the same connectivity model as the production application zone to support lifecycle management of the application. The sensitivity of the information processed by the production application determines the information impact level of the CSO and its PA IAW this SRG. While there may be some exceptions based on where the application developers reside, this also applies to DoD application development Zone B when used for the lifecycle management of a production application. Placing all three zones in the same CSO using the same connectivity model and CSSP as the production application zone helps to realize the efficiencies of the cloud and ultimately better protect the application, the information being processed/stored and the DODIN

DoD application development Zone B instantiated in cloud infrastructure must minimally be implemented in a CSP's CSO that has a Level 2 PA to support pre-production application development with developers accessing the zone via the internet. Consideration for implementing Zone B in a Level 4/5 CSO for this purpose, will depend on the sensitivity of the application itself and its code. This is at the discretion of the program's IAM or responsible AO. Again, once pre-production development is complete and if the Zone B is to be used for the lifecycle management of a production application, then it should be implemented in the same CSP/CSO as the production application. While the systems within the Zone B are not required to be STIG compliant and may not be subject to the same HBSS and ACAS requirements as a Zone A or the production zone, the network infrastructure and network transport must be STIG compliant. This includes a properly hardened zone boundary stack to protect the less than secure inside of the zone. This boundary must be monitored and protected by a CSSP.

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 CSOs connected to NIPRNet 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 or an on-premises DoD 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. Additional 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; i.e., these zones will not connect via a BCAP. Zones C and D may or may not be monitored and protected by a CSSP, however a CSSP must be aligned to receive incident reports and perform incident response.

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

5.14.1 Workstation Connectivity to Cloud Based T&D Zones

Workstation connectivity to all T&D zones instantiated in the cloud will use remote connectivity methods as a result of the nature of Cloud. The different zones require different types of workstations and remote connectivity models. The options are as follows:

- Application test zone A is accessed in the same manner as the production application.
    - Workstations are NIPRNet connected. As with the production application, STIGed government furnished equipment (GFE) must be used to manage the environment and test the application.
- Application development Zone B connectivity:
    - Zone B is in the same CSO as the associated Zone A and production zone (commercial off-premises or DoD private on-premises) supporting lifecycle management of the production application:
        - If the development workstations are NIPRNet connected, as with the production application, STIGed government furnished equipment (GFE) must be used to manage the environment and test the application. A remote terminal solution may be used (e.g., Citrix, Terminal Services (bastion host)). A VPN is only required for tunneling sensitive data.
    - Zone B is in a separate CSO from the associated Zone A and production zone supporting pre-production application development:
        - Commercial off-premises CSO with off-premises contracted developers: Non-GFE may be used across the internet using a VPN or encrypted protocols.
        - Commercial off-premises CSO with on-premises DoD or contracted developers: Zone B must be configured behind its own firewall. A VPN must be used to access the Zone. STIGed GFE must be used due to NIPRNet connectivity. A remote terminal solution is also required after the VPN has been established into the Zone B environment (e.g., Citrix, Terminal Services (bastion host)) where the local WS cannot be compromised from the windowed view of the systems in the zone. The path may be via the IAPs/internet or BCAP/private connection
- T&D/Research Zones C and D:

- Typically, workstations accessing a zone D must do so from within the zone, or from the coupled zone D in a Zone C construct. Cloud presents several different scenarios as follows:

  - Zone D or all portions of a Zone C are instantiated in an internet-connected CSO: workstations connect via the internet. NIPRNet connectivity is generally precluded except for dedicated hardware connecting via a dedicated network or segmented NIPRNet path using VLANs, VRFs, and/or VPNs.

  - One or more Zone D enclaves of a Zone C construct are physical zone D enclaves on DoD premises: All portions of the Zone C including those portions implemented in an off-premises CSO must be accessed from workstations within the Zone C (i.e., the physical zone D enclaves). In this scenario there should be no need for remote access from outside the Zone D or C.

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)*[93] 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[94] [95], 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 use 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.

While the use of non-standard ports for application and/or system to system connectivity, which may be an effective means of mitigating application-specific vulnerabilities, any such usage must be reflected on a DoD PPSM vulnerability assessment (VA) and on the CAL. Such use cases that

[93] DoDI 8551.01: http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf

[94] PPSM Office Cyber Exchange page: http://iase.disa.mil/ppsm/Pages/index.aspx

[95] PPSM Office Public page: http://disa.mil/network-services/Enterprise-Connections/PPSM

cross DISN boundaries must be submitted by the Mission Owner to the PPSM CCB/TAG for assessment and approval.

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. 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 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 use 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 use 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 D-2. 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)[96] 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 cybersecurity defense community tasked with protecting the DODIN, DoD information, and the mission owners cloud based systems/applications.

5.17.2 DoD DMZ Whitelist

The DoD DMZ Whitelist implementation supports USCYBERCOM's TASKORD 12-0371 and subsequent FRAGOs which support the operation of the DoD DMZ program. If all or a portion of the mission owners cloud-based level 4/5 systems/applications connected through the BCAP are to be internet accessible, traffic is required to traverse the DISN IAPs. The system's/application's 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. Such traffic and IP addresses may be blocked if not registered in the whitelist.

Mission owners using IL4/5 I/PaaS CSOs connected to NIPRNet via the BCAP that need all or a portion of their application to be accessible from the internet are responsible for obtaining separate IP ranges for the internet-facing portion from those used for NIPRNet access and for registering the internet-facing addresses in the DMZ whitelist.

Mission owners using IL4/5 P/SaaS CSOs (where they do not have control over the environment) connected to NIPRNet via the BCAP that need all or a portion of their application to be accessible from the internet are responsible for assisting the CSP in obtaining separate IP

[96] SNAP: https://snap.dod.mil/gcap/home.do

Connection Approval: http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Approval

ranges for the internet-facing portion from those used for NIPRNet access and for registering the internet-facing addresses in the DMZ whitelist.

The DMZ whitelist can be found on SIPRNet at https://niprdmzwhitelist.csd.disa.smil.mil/home.aspx. There is a whitelist users guide available via the "Help" link. Mission owners may need to 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)[97] as directed in DoD CIO annual IT budget guidance for each used 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.

As part of the CSO's DoD PA assessment package (if not already provided for the FedRAMP P-ATO or Agency ATO), 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.

[97] 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

5.19 Electronic Mail Protections

CSPs that operate/offer email servers/services must provide for appropriate email protections within the CSO. Mission owners must use these services or provide for alternate capabilities when contracting for email services. Such protections will include, but may not be limited to, email hygiene or scanning for and elimination of malicious content and spam filtering as a minimum.

5.19.1 Electronic Mail Protections IAW TASKORD 12-0920

This section addresses compliance with US CYBERCOM Task Order (TASKORD) 12-0920 regarding SMTP traffic between email systems whether they be a CSO or are agency provided.

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 use 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.

6. CYBERSPACE DEFENSE AND INCIDENT RESPONSE

NOTICE: This release of the CC SRG has been coordinated with the new cyberspace defense lexicon defined in DoD Joint Publication 3-12 (R), "Cyberspace Operations" and DoDI 8530.01, “Cybersecurity Activities Support to DoD Information Network Operations”. Additionally, due to publication of the DoDI 8530.01 and the replacement of the DRAFT Cloud CND CONOPS (rescinded) with DRAFT DoDM 8530.01, “Cyberspace Activity Support to DODIN Operations and Defensive Cyber Operations – Internal Defensive Measures (DCO-IDM)” all releasable content from DoDM 8530.01 applicable to CSPs will be included in a subsequent release. Mission owners and others will refer to the DoDM 8530.01 when published.

Cyberspace defense addresses the defense and protection of networks and information systems (ISs), detection of threats, and response to incidents. Cyber situational awareness improves the quality and timeliness of collaborative decision-making regarding the employment, protection, and defense of DoD systems and data. This section addresses critical cyberspace defense actions; roles and responsibilities; incident reporting and response; and other cybersecurity processes.

6.1 Overview of Cyberspace Defense

DoD operates a cybersecurity structure as defined in DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations”. The structure consists of United States Cyber Command (USCYBERCOM) and Joint Forces Headquarters (JFHQ-DODIN) at the top organizational level and a network of Cybersecurity Service Providers (CSSPs) that have been accredited by USCYBERCOM IAW DoD policy. DoD integrates and employs a number of cybersecurity activities to support DODIN operations and DCO internal defensive measures in response to vulnerabilities and threats, including (1) vulnerability assessment and analysis (VAA); (2) vulnerability management (VM); (3) malware protection (MP); (4) continuous monitoring (CM); (5) cyber incident handling (IR); (6) DODIN user activity monitoring (UAM) for the DoD Insider Threat Program; and (7) warning intelligence and attack sensing and warning (AS&W). Contracts, MOAs, support agreements, international agreements, or other applicable agreements must identify specific operations responsibilities, cybersecurity requirements, protection requirements for DoD data, and points of contact for mandatory reporting of security incidents. Given the requirement for cybersecurity compliance, cloud service provider, cybersecurity service provider and the mission owner security responsibilities should be clearly documented in contract or service level agreement.

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 mission owner requirement as identified by policy. However, in a SaaS environment the operating system is managed by the CSP, as such the CSP would be required to apply operating system patches.

6.2 Concept Changes for Information Impact Levels for Cloud Computing

With the move to commercial cloud computing, the DoD will need to deploy modified network defense capabilities and processes specific to the cloud environment. 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. If the boundary defense is not implemented by the CSP, then the mission owner will be responsible and accountable and must coordinate with their DoD CSSP, who will coordinate with JFHQ-DODIN, for appropriate boundary defense. Protection capabilities supporting the mission system at the system/host/application level will be provided by a combination of the CSSP, mission system administrators, and the CSP (especially for SaaS). Refer to Section 5.10.6, *Mission Owner System/Application Requirements using IaaS/PaaS* for related boundary requirements. CSPs are expected to protect their SaaS CSOs (and PaaS CSOs where the Mission Owner does not have control) by applying the appropriate boundary protections and cyber defense services. Refer to Section 5.10.3, *CSP Service Architecture* and subsections for additional information and CSP requirements for all service models I/P/SaaS.

Impact 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 impact level 4 and above data, the DISN boundary is essentially extended through a connection between an authorized 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; the mission administrators or owners; or the CSSPs that are supporting the monitoring of the mission and the boundary connection. All entities must work together to quickly investigate and respond to incidents. The protection of a DoD BCAP is supported by organizations performing boundary cyberspace actions.

6.2.1 Boundary Cyberspace Defense Actions

Boundary cyberspace defense (BCD) Actions monitor and defend the connections to/from CSPs into the DISN via an authorized BCAP. BCD Actions guard against the risk that each CSP interconnection poses to the DODIN individually, as well as cross-CSP analysis for all connections flowing through an individual BCAP. While these actions focus on the connections through a particular BCAP, cross-BCAP analysis is warranted to determine if a threat extends beyond a single CSP or BCAP.

6.2.2 Mission Cyberspace Defense Actions

Mission cyberspace defense (MCD) Actions performed by the DoD CSSPs provide services to mission owners' cloud-based mission systems/applications and virtual networks. Organizations performing MCD Actions may provide services to cloud-based mission systems/applications and virtual networks instantiated in multiple CSPs and multiple CSOs[98]. While some of these

[98] DoD CIO Memo: https://dl.cyber.mil/cloud/pdf/DoD-CIO-Memo-CS-Activities-Perf-for-Cloud-Serv-Activ-Offerings.pdf

services are mandated to be delivered by the CSSP, other MCD actions may be delivered by a third-party cybersecurity provider, to include the CSP. Wherever the latter is true, the coordination between the third-party cybersecurity provider and the CSSP needs to be explicitly documented in the mission owner SLA. MCD Actions will typically be executed by the CSSP used by the mission owner's component for their non-cloud-based ISs; however, mission owners can choose to use and fund any certified CSSP for execution of MCD Actions; C2 relationships between organic CSSPs and otherwise employed forces will need to be coordinated by the mission owner.

6.3 Cyberspace Defense Actions

The following is a list of cyberspace defense actions and their responsibilities as it relates to cloud operations.

- **DODIN Cyberspace Defense (DCD) Actions:** The primary objective of the organization that performs DCD Actions is to oversee a coordinated response to DODIN-wide attacks. DCD builds a broad picture of the operating environment across mission owners, MCDs, BCDs, CSOs, and CSPs. The DCD identifies patterns of incidents or events, consolidates related incident tickets, directs mitigations, and assigns DODIN Cyber Protection Teams (CPTs) to focus efforts on a specific threat or adversary. Specific cyberspace defense actions include:
  - Protect the DODIN and DoD mission systems in commercial cloud infrastructure through cross-BCAP correlation and analysis of events/data
  - Direct or recommend cybersecurity actions regarding DODIN-wide incident and system health reporting involving a BCAP or CSP
  - Establish and maintain external communications with the CSP for DODIN-wide incidents and ensure internal DoD communications are established between all entities, which includes the MCD and BCD
  - Interface with US-CERT to obtain relevant CSP information; ensure cross-sharing of information across all organizations performing BCD/MCD Actions
- **Boundary Cyberspace Defense (BCD) Actions:** The primary objective of organizations that perform BCD Actions is to protect the Defense Information Systems Network (DISN) from events or incidents that use public, private, hybrid, or community clouds. BCD Actions support CSSPs performing MCD Actions in their objectives of defending DoD systems, applications, and data hosted in the cloud. specific cyberspace defense actions include:
  - Protect the DISN via the BCAP
  - Provide timely access to BCD-collected indications and warnings relevant to organizations performing MCD Actions
  - Support DCD Actions to identify correlations between related events or incidents that impact multiple Mission Owners, CSOs, or CSPs

- **Mission Cyberspace Defense (MCD) Actions:** The primary objective of organizations that perform MCD Actions is to defend mission owners' systems, applications, and data hosted in the Cloud. MCD Actions are performed by cybersecurity service providers (CSSPs) on behalf of their organic organizations and subscribers. Specific cyberspace defense actions include:

  - Analyze cyber incidents and events for mission owners
  - Monitor, protect, and defend mission owners' cloud-based systems, applications, and virtual networks in the CSP's CSOs infrastructure
  - Monitor, protect, and defend mission owners' cloud-based data in the CSO
  - Defend all connections to the CSO, whether via BCAP, Virtual Private Network (VPN), IAP, direct internet access to public servers, or other
  - Monitor privileged actions (e.g., cloud management or mission owner application administration) and monitor for events or incidents against the mission owner applications (e.g., Structured Query Language (SQL) injection)
  - Support DCD efforts to identify correlations between related events or incidents that impact multiple mission owners, CSOs, or CSPs
  - Ensure internal DoD communications are established between all entities which include the mission owner and other organizations performing MCD and BCD Actions
  - Provide visibility and awareness of cyber incidents or events impacting mission owner systems, applications, virtual networks, and data to JFHQ-DODIN

6.4 Cyberspace Defense Roles and Responsibilities

The following is a list of the cyberspace defense roles and responsibilities as they relate to cloud operations.

- **JFHQ-DODIN:** JFHQ-DODIN will perform DCD actions and has direct tasking authority over DoD Components. JFHQ-DODIN, as part of USCYBERCOM, has legal authority to collaborate with entities external to DoD, such as the United States Computer Emergency Readiness Team (US-CERT)

- **DoD Components:** Service cyber components, defense agencies, and DISA may perform MCD Actions in support of their mission owners; and BCD actions when they have the responsibility of operating, monitoring, and maintaining a BCAP

- **Mission Administrators:** Administrators of mission owner's cloud-based systems, applications, and virtual networks; responsible for:

  - Following the directives and orders from the mission owner

- 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 stated in Section 6.1, Overview of Cyberspace Defense, some DoD Components might transfer some or all of these responsibilities to organizations performing MCD actions

- **Cloud Service Provider (CSP):** CSPs provide their own cyberspace defense services for the underlying infrastructure made available for their customer's (DoD mission owner's) applications, systems, and virtual networks (SaaS, PaaS, IaaS). In effect, the CSP will function as an extension of the mission owner, who has transferred responsibility for maintaining that infrastructure to the CSP through an SLA for those services. At a minimum, CSPs responsibility is defined in the DoD CIO memorandum, "Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings", Attachment 1[99].

- **Mission Owners:** Individuals/organizations responsible for the overall mission environment, ensuring that the functional and cyberspace defense requirements of the system are being met. Mission owners, as the CSO subscribers to the CSPs, have a contractual relationship to the CSPs. Mission owners can optionally expand cyberspace defense relevant reporting to their organizations performing MCD and BCD actions by including such language in their service level agreements (SLAs). At a minimum, mission owners responsibility is defined in the DoD CIO memorandum, "Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings", Attachment 1[100].

6.5 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. Refer to incident.

- **Incident**: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information

[99] DoD CIO Memo: https://dl.cyber.mil/cloud/pdf/DoD-CIO-Memo-CS-Activities-Perf-for-Cloud-Serv-Activ-Offerings.pdf

[100] DoD CIO Memo: https://dl.cyber.mil/cloud/pdf/DoD-CIO-Memo-CS-Activities-Perf-for-Cloud-Serv-Activ-Offerings.pdf

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, 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[101] (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. USCYBERCOM/JFHQ-DODIN will handle coordination with US-CERT and other entities as appropriate. The DoD incident reporting process is described in Section 6.5.3, *Incident Reporting Mechanism*.

All CSPs actively supporting DoD missions will be supported by one or more organizations performing MCD Actions. The CSSP contracted to perform MCD Actions will be the DoD point of contact with whom the CSP's operational entity will coordinate responses to incidents affecting the security posture of the CSP and the CSP's cloud service offerings. The organizations performing MCD Actions will coordinate with the organizations performing BCD Actions as appropriate.

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

6.5.1 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 Cyberspace 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 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

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

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 6.5.3, *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 PII data breaches within one hour)
- How and under what circumstances any individuals or entities affected by an incident will be notified and by whom
- Any other special instructions for handling computer security incidents affecting, or potentially affecting US 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

6.5.2 Information Requirements, Categories, Timelines, and Formats

Defending DoD missions and systems is a shared responsibility that requires all entities (CSPs, organizations performing MCD or BCD actions, 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 CAP):

- CSP personnel through monitoring of their CSO (especially for PaaS/SaaS);
- Mission administrators or owners (includes the CSP for PaaS/SaaS);
- Supporting organizations performing MCD Actions through monitoring;
- Supporting organizations performing BCD Actions via BCAP monitoring.

All entities must work together to quickly investigate and respond to events and incidents.

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[102])
- 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, D.C., Los Angeles, California)
- 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 must 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 organizations performing MCD/BCD Actions. 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 DoD organizations performing CSSP.

6.5.3 Incident Reporting Mechanism

DoD CSSP's 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(c) as updated for Cloud Computing when finalized.

Level 2/4/5 commercial CSPs will report all incidents via the online defense industrial Base (DIB) cyber incident collection format (ICF)[103] . Use of the online format is preferred. Access 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 the DoD missions affected by the incident when distributing this report. The DoD mission owners and security POCs (CSSPs) and other entities that might have a role, for example contract managers, etc. Once the report is received, the CSSP performing MCD actions will initiate the DoD reporting process via JIMS.

---

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

[103] DIBNet CS/IA Portal: http://dibnet.dod.mil/

In the event of an incident against a classified system, 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 organization performing MCD Actions 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 cyberspace defense information may be used, provided 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

6.5.4 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, if possible, determine 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*[104].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)

6.5.4.1 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 organization performing MCD actions for analysis in addition to any other analysis organization employed by the CSP. The means of submission will be coordinated with the organization performing MCD Actions. The DoD cyberspace defense community will use their analysis to 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.

[104] NISTIR 8006: http://csrc.nist.gov/publications/PubsDrafts.html

Corresponding Security Controls: SI-3 (10)

6.5.4.2 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.

Under IaaS, when a mission owner discovers a cyber-incident has occurred within their systems/applications/virtual networks, they will work with their organization performing MCD actions 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 webpage[105], 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 organization performing MCD actions is required to have and use similar procedures and tools. The mission owner and/or the organization performing MCD Actions 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, the organization performing MCD actions, 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.

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 organization performing MCD Actions 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,

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

and protect functions. The CSP will then do a dual report to share their results with the mission owner and security POC (CSSP) performing MCD actions.

Under SaaS, the CSP must perform the capture, preserve, and protect functions. The CSP will then share their results with the mission owner's CSSP performing MCD actions.

All captured incident information is digital evidence. Upon collection of digital evidence, 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 from modification or deletion, 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 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 forensic analysts 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 except 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/CSSP performing MCD.

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

6.5.4.3 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 website 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

6.5.4.4 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.

6.6 Warning, Tactical Directives, and Orders

USCYBERCOM or JFHQ-DODIN disseminates warnings, tactical directives, and orders to the organizations performing BCD and MCD Actions. The organizations performing BCD and MCD actions will analyze them for their applicability to individual mission owners and CSPs, and then, as appropriate and applicable, communicate the requirements to these same mission owners and CSPs. CSPs will coordinate with the organizations performing MCD actions and mission owners to implement directives and countermeasures in compliance with timelines identified. Upon completion of actions, the organization(s) performing MCD and BCD actions will report compliance back to JFHQ-DODIN and USCYBERCOM.

CSPs must be able to receive, act upon, and report compliance with directives and notifications sent by the organization performing MCD Actions on behalf of the mission owner, as required by FedRAMP selected security control SI-5.

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

Understanding existing vulnerabilities and risks within the enterprise is a key component in performing effective cyberspace 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 organizations performing MCD and BCD Actions for their collective use in providing cyberspace 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

6.8 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 organizations performing MCD actions 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 organization performing MCD actions to the organization performing BCD Actions to enable broader situational awareness. Mission owners and administrators are responsible for the same notifications to the organizations performing MCD actions when the ASI is under their control.

6.9 PKI for Cyberspace Defense Purposes

The DoD PKI program provides assurances of an individual's identity, which is important in sharing information regarding C2 and cyberspace defense actions. This section outlines requirements for establishing trusted identities for CSP personnel communicating securely with DoD cyberspace defense personnel. Once an incident is reported through the process identified in Section 6.5.3, Incident Reporting Mechanism or encrypted email is to be used as the subsequent communications method, DoD PKI certificates will be required as follows:

- ***Impact Levels 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 Cyber Exchange PKI/ECA webpage[106]and PKI/PK Enabling (PKE) webpage[107]. 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 cyberspace defense personnel will use SIPRNet tokens/certificates to communicate with DoD via encrypted email.

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

[106] Cyber Exchange PKI/ECA page: http://iase.disa.mil/pki/eca/Pages/index.aspx

[107] Cyber Exchange PKI/PKE Page: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx

The Defense Industrial Base Cybersecurity/Information Assurance Program[108] (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, which 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 detailing classified and unclassified cyber threat information, including mitigation strategies. DIB CS/IA program membership is voluntary, although cyber incident reporting as described in Section 6.5.3, *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 Cyberspace Defense communications architecture and receive unclassified CYBERCOM notifications via established channels.

[108] 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. 22 Code of Federal Regulations (CFR), 22 CFR 120.17 – Export,
https://www.gpo.gov/fdsys/pkg/CFR-2004-title22-vol1/pdf/CFR-2004-title22-vol1-sec120-17.pdf
6. 22 Code of Federal Regulations (CFR), 22 CFR 120.-130 International Traffic in Arms Regulations Part 123 - Licenses for the Export of Defense Articles,
https://www.pmddtc.state.gov/regulations_laws/itar.html
7. 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
8. Executive Order 13526: Classified National Security Information, dated 29 December 2009.
http://www.archives.gov/isoo/policy-documents/cnsi-eo.html
9. Executive Order 12829 – National Industrial Security Program, January 1993.
http://www.archives.gov/isoo/policy-documents/eo-12829.html
10. Executive Order 13556 - Controlled Unclassified Information.
https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
11. 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
12. 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
13. 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

14. 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

15. NIST SP 500-292: NIST Cloud Computing Reference Architecture, dated September 2011.
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

16. 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.

17. 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

18. 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

19. NIST SP 800-88, Revision 1: Guidelines for Media Sanitization, dated September 2012.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

20. 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

21. 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

22. NIST SP 800-145: The NIST Definition of Cloud Computing, dated September 2011.
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

23. 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

24. 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

25. CNSS Instruction 4009: National Information Assurance (IA) Glossary, dated 30 April 2010.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm

26. 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

27. 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

28. CNSS Instruction No.1253F, Attachment 6: Privacy Overlay dated 20 April 2015.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm

29. 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

30. DoD Instruction 8500.01: Cybersecurity, dated 14 March 2014.
http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

31. 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

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

33. DoD Instruction 8550.01: DoD Internet Services and Internet-Based Capabilities, September 11, 2012.
http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf

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

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

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

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

38. 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

39. 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

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

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

42. 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

43. 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

44. 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

45. 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

46. 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

47. 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

48. DoD Manual 5200.02: Personnel Security Program, dated February 1996.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002m.PDF

49. 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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix B. **Glossary**

B.1. Cloud Terminology

This section is organized by topic.

Cloud Service Provider (CSP): An organization, commercial or Private, that offers/provides Cloud Services. Unqualified use of the term refers to any or all cloud service providers, DoD or non-DoD.

Commercial CSP: A non-federal government non-DoD organization offering cloud services to the public and/or government customers as part of a business venture, typically for a fee with the intent to make a profit.

Federal Government CSP: A federal government organization offering cloud services which may be owned and operated by the federal government or a contractor for the benefit of the federal government.

DoD CSP: A DoD organization offering cloud services which may be owned and operated by DoD or a contractor for the benefit of the DoD.

Non-DoD CSP: A commercial CSP or federal government CSP.

Cloud Service Offering (CSO): refers to a CSP's product or service offering. In other words, a CSO is the actual Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) solution available from a CSP. A CSP may provide multiple CSOs (e.g., Microsoft O-365 (SaaS) and Azure (I/PaaS)). CSO also refers granularly to optional services or software available within any of the service types (e.g., one or more specific database applications optionally available for customer usage under PaaS).

- **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)."*

- **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."*

- **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."

Community Cloud: A multi-tenant cloud in which services are provided for the exclusive use of a specific group or type of independent customer organizations.

Federal Government Community Cloud: A community cloud offered for use by multiple federal government organizations (which include the DoD). Resources providing the cloud services must be dedicated to federal government use and require physical separation from non-Federal customers.

Private Cloud: A single or multi-tenant cloud in which services are provided for the exclusive use of a specific customer organization.

DoD Private Cloud/CSO: a DoD Community Cloud or CSO in which services are provided for the exclusive use of one or more DoD customer organizations; 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.

DoD Cloud Service Catalog[109]**:** The repository of all CSOs that have been awarded a DoD PA and have security packages available for DoD components to leverage.

DoD Component: A DoD Service or agency including their sub-elements/commands/organizations.

DoD Off-Premises: A facility (building/container) or IT infrastructure is off-premises if it is NOT physically or virtually on DoD owned or controlled property (i.e., on-premises physically or virtually). Refer to Section 5.2.1.1, *DoD Off-Premises vs. On-Premises vs. Virtually On-Premises* for additional details.

DoD On-Premises: A facility (building/container) or IT infrastructure is on-premises if it is physically on DoD owned or controlled property. That is, it is within the protected perimeter (walls or "fence line") of a DoD installation (i.e., base, camp, post, or station (B/C/P/S) or leased commercial space) which is under the direct control of DoD personnel and DoD security policies. Refer to Section 5.2.1.1, *DoD Off-Premises Vs On-Premises Vs Virtually On-Premises* for details.

---

[109] 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)

DoD Virtually On-Premises: A IT infrastructure located in a physically off-premises location such as a federal government or commercial data center (i.e., facilities under the direct control of non-DoD personnel using non-DoD security policies) may be considered virtually on-premises under specific conditions. These conditions apply certain physical security controls and extend the DISN accreditation boundary. In essence this construct virtually extends the DoD protected perimeter or "fence line" around the infrastructure. Refer to Section 5.2.1.1, *DoD Off-Premises vs. On-Premises vs. Virtually On-Premises* for details and requirements.

Mission Owner (MO): Mission owners are 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 fulfillment of their 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 responsible to the information owner and the information system's AO. The information owner, in addition to owning the information and all associated derivatives, is responsible for ensuring the data that is migrated to the cloud is at the appropriate security level having the approval of their risk management executive/AO.

B.2. General Terminology

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."*

C/CE (Control/Control Enhancement): 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.

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

CSSP: Cybersecurity service provider. Defined in DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations.

Dedicated infrastructure: Refers to the cloud service infrastructure being dedicated to serving a single customer organization or a specific group of customer organizations (e.g., a specific community).

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. Refer to 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.

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."*

Provisional Authorization (PA): A pre-acquisition type of Risk Management Framework Information System Authorization used by DoD and FedRAMP to pre-qualify Commercial CSOs to host Federal Government and/or DoD information and information systems. PAs are to be used by Federal and DoD Cloud Mission Owners during source selection and subsequent system authorization under RMF. Refer to Section 2.6 - *DoD Provisional Authorization.*

RMF: Risk Management Framework. As described in NIST SP 800-37, RMF is a six-step risk based approach to information system security, the purpose of which is compliance with various public laws including FISMA. The RMF replaces the traditional certification and accreditation C&A processes.

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."*

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 C-1 provides a summary of the major roles and responsibilities in implementation of the CC SRG.

Table C-1: 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 Boundary Cloud Access Point (BCAP). • Provide Boundary Cyberspace Defense (BCD) capabilities. • 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 CSSP 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 cybersecurity services 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

Role	Responsibility
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 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
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 AO	• Official approving PA for a CSP's Service Offerings for DoD use
DoD Component AO	• Official approving ATOs for Mission Owner's systems/applications • Reviews PA documentation to understand residual risk

Role	Responsibility
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 Mission Cyberspace Defense (MCD) Service Provider is identified and funded • Performs end-point Cyberspace Defense for their mission systems/applications • Ensures CSP requirements for Cyberspace 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 C2 direction addressing the protection of the network, detection of threats, and response to incidents.
Cybersecurity Service Provider (CSSP)	• Provides cybersecurity services for the protection of the network, detection of threats, and response to incidents.
Organizations Performing Boundary Cyberspace Defense (BCD) Actions • DoD CSSPs	• Monitor and defend the connections to/from off-premises CSPs at the Boundary Cloud Access Point (BCAP) • Provide cross-CSP analysis capabilities or entities • Communicate with organizations performing DCD, BCDs, and MCDs Actions. • Provide MCDs timely access to BCD-collected indications and warnings relevant to MCD subscribers.
Organizations Performing Mission Cyberspace Defense (MCD) Actions • DoD CSSP	• Provide Cyberspace Defense services to specific Mission Owner's systems/applications and virtual networks • Serve as the DoD Cyberspace Defense point of contact for the Mission Owner • Communicate with organizations performing DCD, BCDs, and MCDs Actions, and Mission Owners.

Appendix D. **CSP Assessment Parameter Values for PA**

Table D-1 provides a listing of the FedRAMP+ C/CEs **that require parameter values and the FedRAMP C/CE for which DoD requires adjustment.** 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.

Note: The number of parameter values presented in Table D-1has been reduced in this release of the CC SRG to foster greater reciprocity at Level 4 and 5 with the FedRAMP Moderate Baseline (MBL).

Note: For Level 6, the application of the CNSSI 1253 Classified Information Overlay will modify some of the values of C/CE presented in the tables below as well as other C/CE not listed. Overlay values take precidence.

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 system security plan (SSP) and accepted by the DISA AO as reflected in the PA or negotiate for alrernate values and include them in their contract/SLA.

Table D-2 provides a listing of only the C/CEs listed in Table 5-2: Security Controls/Enhancements to be addressed in the Contract/SLAthat 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 D-2* 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.

NOTICE: In addition to parameter values required for the implementation of FedRAMP+ C/CE, *Table D-1* contains FedRAMP Moderate C/CE where the value is non-existent or requires adjustment. Many of the parameter value adjustments are sourced from the FedRAMP HBL because DoD believes the value is relevant and required at the Moderate level. These values will be submitted to the FedRAMP PMO for potential adjustment. Such adjustment, however, may not occur until NIST 800-53 rev5 is released and the FedRAMP baselines are adjusted to this new release.

Table D-1: FedRAMP+ Control/Enhancement Parameter Values for PA Assessment

Control/Enhancement Text	Value
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-06 (01) MBL: Use HBL value; HBL: Defer to FedRAMP value
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-06 (07) MBL based PA: AC-6 (7)(a)-1 at a minimum, annually AC-6 (7)(a)-2 all users with privileges HBL based PA: Defer to FedRAMP Value
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-06 (08) MBL based PA: AC-6 (8) [any software except software explicitly documented] HBL based PA: Defer to FedRAMP Value
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-08 For DoD usage CSO must provide for MO compliance with DoD banner requirements. As such, a. The CSO must have a customer configurable capability to support a logon banner having a minimum of 1300 characters that is displayed and acknowledged before any logon prompt offered to privileged and non-privileged customer users for access to customer's services. c.1. Refer to a. For CSO customer privileged user account portal access not dedicated to one customer, Defer to FedRAMP MBL/HBL guidance. Mission Owner Guidance: Configure the CSO provided customer logon banner capability and any Mission Owner provided logon capability to mission applications, virtual machines, databases, etc. IAW DoDI 8500.01 Encl. 3, para 9.a.(1)(d) for all privileged and non-privileged customer users that must logon Source: DoD RMF TAG IG&VP documentation. adjusted for Cloud

Control/Enhancement Text	Value
AC-17 (3); ACCESS CONTROL; Remote Access - Enhancement: Managed Access Control Points The information system routes all remote accesses through **[Assignment: organization-defined number]** managed network access control points. References: None.	AC-17 (03) Level 4/5: Off-Premises CSP infrastructure must support a private connection service to connect to DoD customers via one or more DISN Boundary Cloud Access Points (BCAPs). In production, the CSP infrastructure will serve NIPRNet based customers via a BCAP connection. Level 4/5: On-Premises Commercial CSP infrastructure must connect to DoD customers via one or more Internal DODIN Cloud Access Points (CAPs) if the CSO infrastructure is mandated off-premises.
AC-18 (1); ACCESS CONTROL; Wireless Access - Enhancement: Authentication And Encryption The information system protects wireless access to the system using authentication of **[Selection (one or more): - users; - devices]** and encryption. References: None.	AC-18 (01) IF wireless access is permitted in the CSO infrastructure, both users and devices must be authenticated.
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-03 (04) MBL based PA: AT-3 (4) [malicious code indicators as defined by organization incident policy/capability] HBL based PA: Defer to FedRAMP Value
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-02 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 IG&VP documentation.
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 (01) Parameter 1: MBL based PA: AU-12 (1) [all network, data storage, and computing devices] HBL based PA: Defer to FedRAMP Value. Parameter 2: The time tracking tolerance defined in AU-8

Control/Enhancement Text	Value
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-02 DoD value(s) assessed for DoD Level 4/5/6 PA b. Defer to FedRAMP value d. individuals or roles to include FedRAMP PMO, the DISA A&A/SCA team, the customer's AO and CSSP
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-03 No Entry - Defer to FedRAMP values
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-03 (01) No Entry Rationale: U-NSS not supported at IL4
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-03 (05) For HBL based PA: Defer to FedRAMP Value. For MBL based PA: Use DoD or HBL value as follows: Selection: - deny-all, - permit by exception Param. 2: any systems requiring external connectivity Source: FedRAMP HBL and DoD RMF TAG IG&VP documentation.
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-02 (03) MBL based PA: CM-2 (3) [organization-defined previous versions of baseline configurations of the previously approved baseline configuration of IS components] HBL based PA: Defer to FedRAMP Value.

Control/Enhancement Text	Value
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-03 (04) MBL based PA: CM-3 (4) Configuration control board (CCB) or similar (as defined in CM-3) HBL based PA: Defer to FedRAMP Value.
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-03 (06) MBL based PA: CM-3 (6) All security safeguards that rely on cryptography HBL based PA: Defer to FedRAMP Value.
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-05 (04) MBL based PA: use FedRAMP HBL/DoD Value. IA-5 (4) [complexity as identified in IA-5 (1) Control Enhancement Part (a)] HBL based PA: Defer to FedRAMP Value.
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-02 MBL based PA: use FedRAMP HBL or DoD Value. IR-02 a. 30 working days. c. At least annually. HBL based PA: Defer to FedRAMP Value.
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-04 (08) Param. 1: MBL based PA: IR-4 (8) [external organizations including consumer incident responders and network defenders and the appropriate CIRT/CERT (such as US-CERT, DOD CERT, IC CERT)] HBL based PA: Defer to FedRAMP Value. Param. 2: Incident information as defined in Section 6.4 - Cyber Incident Reporting and Response
IR-9 (2); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Training The organization provides information spillage response training **[Assignment: organization-defined frequency]**. References: None.	IR-09 (02) MBL based PA: use FedRAMP HBL/DoD Value. IR-9 (2) [at least annually] HBL based PA: Defer to FedRAMP Value.
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-02 MBL based PA: use FedRAMP HBL/DoD Value. MP-2-1 [any digital and non-digital media deemed sensitive] HBL based PA: Defer to FedRAMP Value.

Control/Enhancement Text	Value
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-06 MBL based PA: MP-6(a)-2 [techniques and procedures IAW NIST SP 800-88 and Section 5.9: Reuse and Disposal of Storage Media and Hardware] HBL based PA: Defer to FedRAMP Value.
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 MBL based PA: SA-12 [organization and service provider-defined personnel security requirements, approved HW/SW vendor list/process, and secure SDLC procedures] HBL based PA: Defer to FedRAMP Value.
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-07 (12) MBL based PA: use FedRAMP HBL/DoD Value. SC-7(12)-1 [Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall] HBL based PA: Defer to FedRAMP Value.
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-08 (02) No Entry
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 (01) MBL based PA: use FedRAMP HBL/DoD Value. SC-28 (1)-2 [all information system components storing customer data deemed sensitive] HBL based PA: Defer to FedRAMP Value.
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-02 (06) All upgraded/replaced software and firmware components that are no longer required for operation Source: DoD RMF TAG IG&VP documentation. ----------

Table D-2: Parameter Values for SLA Controls/Enhancements Listed in Table 5-2

As noted in Section *5.1.6 Security Controls/Enhancements to be optionally addressed in the Contract/SLA* above, the Mission Owner has the option to tailor in any of the C/CE in *Table 5-2: Security Controls/Enhancements Optionally Addressed in the Mission Owner's Contract/SLA* above and add them to their contract/SLA with the CSP. Additionally, the Mission Owner is responsible for defining any parameter values required. This table provides example values as defined for DoD by the DoD RMF TAG for the DoD CIO that the Mission Owner may choose to use. This table only contains those SLA C/CE that require parameter values.

Control/Enhancement Text	Value
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.	[Value not Defined; To be defined by CSP or Mission Owner]
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 ----------

Control/Enhancement Text	Value
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.	[Value not Defined; To be defined by CSP or Mission Owner]
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**

Control/Enhancement Text	Value
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:** IAPs, 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. Refer to 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 E-1 - *FedRAMP M C/CE Modified or Required by Regulation*
- Table E-2- *FedRAMP+ C/CE Modified or Required by Regulation*
- Table E-3 - *Privacy Overlay C/CE Not Included In FedRAMP M* or FedRAMP+
- Table E-4 - *PII/PHI Parameter Values for FedRAMP and FedRAMP+ C/CE*
- Table E-5 - *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 E-1: 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
MP-07	FR.M	X	X		+GVR	+GVR	

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
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	
SI-11	FR.M	X	X	+VR	+VR	+VR	+VR
SI-12	FR.M	X	X	+EGR	+EGR	+EGR	+EGR

Table E-2: 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 E-3: 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

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
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	
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	

C/CE	SRG Type	L4	L5/6	PII L	PII M	PII H	PHI
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 E-4: PII/PHI Parameter Values for FedRAMP and FedRAMP+ C/CE

Note: This table may modify the parameter values in Table D-1 and Table D-2 when PII/PHI is involved.

Control/Enhancement Text	Value
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

Control/Enhancement Text	Value
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

Control/Enhancement Text	Value
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

Control/Enhancement Text	Value
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…

Control/Enhancement Text	Value
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

Control/Enhancement Text	Value
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

Control/Enhancement Text	Value
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, and 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

Control/Enhancement Text	Value
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 E-5: PII/PHI Parameter Values for C/CE Not Included in FedRAMP M or FedRAMP+

Control/Enhancement Text	Value
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

Control/Enhancement Text	Value
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

Control/Enhancement Text	Value
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