



DRAFT

**DEPARTMENT OF DEFENSE (DOD)
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE (SRG)**

Version 1, Release 0.36

7 December, 2014

**Developed by the
Defense Information Systems Agency (DISA)
for the
Department of Defense (DoD)**

UNCLASSIFIED

This page is intentionally blank.

DRAFT

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DoD, DISA, or DISA Field Security Operations (FSO) of any non-Federal entity, event, product, service, or enterprise.

DRAFT

Table of Contents

1	INTRODUCTION.....	1
1.1	Purpose and Audience.....	1
1.2	Authority.....	2
1.3	Scope and Applicability.....	2
1.4	Security Requirements Guides (SRGs) / Security Technical Implementation Guides (STIGs).....	3
1.5	SRG and STIG Distribution.....	4
1.6	Document Revisions and Update Cycle.....	4
1.7	Document Organization.....	4
2	BACKGROUND.....	6
2.1	Cloud Computing, Cloud Service, and Cloud Deployment Models.....	6
2.2	Cloud Service Provider (CSP).....	6
2.3	DoD Risk Management Framework (DoD RMF).....	6
2.4	Federal Risk and Authorization Management Program (FedRAMP).....	7
3	RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS.....	8
3.1	Assessment of Commercial/Non-DoD Cloud Services.....	8
3.2	Assessment of DoD Provided Cloud Services.....	9
3.3	Cloud Service Offering Risk Management.....	9
3.3.1	Cloud Service Offering (CSO) Risk.....	9
3.3.2	Mission Risk.....	9
3.3.3	Mission System Inheritance.....	10
3.4	CSP Transition from CSM v2.1 to Cloud Computing SRG v1r1.....	10
4	IMPACT LEVELS / SECURITY OBJECTIVES.....	12
4.1	Impact Levels.....	12
4.1.1	Level 1; Unclassified Information approved for Public release:.....	12
4.1.2	Level 2; Non-Controlled Unclassified Information:.....	12
4.1.3	Level 3; Controlled Unclassified Information:.....	12
4.1.4	Level 4; Controlled Unclassified Information:.....	12
4.1.5	Level 5; Controlled Unclassified Information:.....	13
4.1.6	Level 6; Classified Information up to SECRET:.....	13
4.2	Security Objectives (Confidentiality, Integrity, Availability).....	14
5	SECURITY REQUIREMENTS.....	16
5.1	DoD Policy Regarding Security Controls.....	16
5.1.1	DoD use of FedRAMP Security Controls.....	16
5.1.2	DoD FedRAMP+ Controls/Enhancements.....	16
5.1.3	Risk Acceptance for FedRAMP+ Controls/Enhancements at Level 2.....	17
5.1.4	Parameter Values for Security Controls and Enhancements.....	20
5.1.5	Controls/Enhancements to be Addressed in the Contract/SLA.....	20
5.2	Legal Considerations.....	21
5.2.1	Jurisdiction/Location Requirements.....	21
5.2.2	Cloud Deployment Model Considerations / Separation Requirements.....	21
5.2.2.1	Impact Level 2 Location and Separation Requirements.....	22
5.2.2.2	Impact Levels 4 and 5 Location and Separation Requirements.....	22

5.2.2.3	Impact Level 6 Location and Separation Requirements	22
5.3	Ongoing Assessment.....	23
5.3.1	Continuous Monitoring.....	23
5.3.1.1	CSPs in the FedRAMP Catalog	23
5.3.1.2	3PAO assessed Federal Agency ATO	24
5.3.1.3	DoD Self-Assessed CSPs.....	26
5.3.2	Change Control	27
5.3.2.1	CSPs in the FedRAMP Catalog	27
5.3.2.2	3PAO assessed Federal Agency ATO	29
5.3.2.3	DoD Self-Assessed CSPs.....	30
5.4	CSP use of DoD Public Key Infrastructure (PKI)	30
5.4.1	Identification, Authentication, and Access Control Credentials.....	31
5.4.1.1	Mission Owner Credentials.....	31
5.4.1.2	CSP Privileged User Credentials	33
5.4.2	Public Key (PK) Enabling	33
5.5	Policy, Guidance, Operational Constraints.....	34
5.5.1	SRG/STIG Compliance	34
5.6	Physical and Personnel Requirements	34
5.7	Data Spill	35
5.8	Data Removal/Recovery and Destruction.....	36
5.9	Disposal of Storage Hardware	37
5.10	Architecture.....	37
5.10.1	Cloud Access Point.....	37
5.10.2	Network Planes	38
5.10.3	Network Plane Connectivity.....	38
5.10.3.1	User/Data Plane Connectivity.....	38
5.10.3.2	Management Plane Connectivity	40
5.10.4	CSP Service Architecture	42
5.10.4.1	SaaS.....	43
5.10.4.2	IaaS/PaaS	43
5.10.5	IP Addressing and DNS	44
5.10.6	Mission Owner Architecture using SaaS	44
5.10.7	Mission Owner System/Application Architecture using IaaS/PaaS	45
6	COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE.....	48
6.1	Overview of CND Tiers.....	48
6.2	Concept Changes for Tiers for Cloud Computing	48
6.2.1	Boundary CND	48
6.2.2	Mission CND	49
6.3	CND Roles and Responsibilities.....	49
6.4	Incident Reporting and Response	51
6.4.1	DoD Command and Control and Network Operations Integration	52
6.4.2	Information Requirements, Categories and Timelines	52
6.4.3	Incident Reporting Mechanism.....	54
6.4.4	Incident Reporting Format.....	54
6.5	Warning, Tactical Directives, and Orders.....	55
6.6	Vulnerability Reporting / Plans of Action and Milestones (POA&Ms).....	55

6.7	Notice of Scheduled Outages.....	55
6.8	PKI for CND Purposes.....	55
6.9	CND Operations.....	56
6.10	Vulnerability and Threat Information Sharing	56
6.10.1	Defense Industrial Base Cyber Security / Information Assurance Program.....	56
Appendix A	References	A-1
Appendix B	Definitions.....	B-1
Appendix C	Roles and Responsibilities	C-1
Appendix D	Parameter Values.....	D-1

List of Tables

Table 1 - Potential Impact Definitions for Security Objectives.....	15
Table 2 - DoD FedRAMP+ IA Controls/Enhancements	17
Table 3 - IA Controls/Enhancements to be addressed in the contract/SLA	20
Table 4 - Mission Owner Credentials	32
Table 5 - User/Data Plane Connectivity	38
Table 6 - Management Plane Connectivity.....	40
Table 7 – Incident Categories per Impact Level.....	54
Table 8 - Roles and Responsibilities.....	C-1
Table 9 – Control / Enhancement Parameter Values	D-1

List of Figures

Figure 1 – Notional Division of Security Inheritance and Risk.....	10
Figure 2 – DoD Continuous Monitoring for CSPs with a FedRAMP JAB PA	24
Figure 3 – DoD Continuous Monitoring for FedRAMP CSPs with a 3PAO assessed Federal Agency ATO.....	25
Figure 4 – DoD Continuous Monitoring for DoD Self-Assessed CSPs	26
Figure 5 – DoD Change Control Process for CSPs with a FedRAMP JAB PA.....	28
Figure 6 – DoD Change Control Process for FedRAMP CSPs with a 3PAO assessed Federal Agency ATO.....	29
Figure 7 – DoD Change Control Process for DoD Self-Assessed CSPs	30
Figure 8 – DoD Cloud Incident Response and CND C2 Structure.....	51

This page is intentionally blank.

1 INTRODUCTION

The Department of Defense (DoD) Chief Information Officer (CIO) is committed to accelerating the adoption of cloud computing within the Department and providing an Enterprise Cloud Environment with a well-defined security capability that aligns with Department-wide Information Technology (IT) efficiency initiatives, and federal data center consolidation. Key benefits achieved with cloud computing include increased mission effectiveness and operational efficiencies. Cloud computing enables the Department to consolidate and share commodity IT functions resulting in a more efficient use of resources.

On 26 June 2012, the DOD CIO issued a memo designating DISA as the DOD Enterprise Cloud Services Broker. The [currently draft] DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services* clarifies Broker responsibilities and updates DoD Component responsibilities when acquiring commercial cloud services. One of DISA's key responsibilities is securing the Department of Defense Information Networks (DoDIN) by addressing cybersecurity challenges associated with outsourcing DoD IT and data to commercial and non-DoD clouds.

DISA previously published the concepts for operating in the commercial cloud under the Cloud Security Model. Version 1 defined the overall framework and provided initial guidance for capabilities encompassed in Impact Levels 1 and 2. Version 2.1 added information for Impact Levels 3 through 5. This document, the Cloud Computing Security Requirements Guide (SRG), documents cloud security requirements in a construct similar to other SRGs published by DISA for the DOD. This SRG incorporates, supersedes, and rescinds the previously published Cloud Security Model.

The following terms will be used throughout this document:

- CSP by itself refers to any or all Cloud Service Providers, DoD or non-DoD.
- Non-DoD CSP will refer to a commercial or Federal Government owned and operated CSP.
- DoD CSP will refer to a DoD owned and operated CSP.
- CSO refers to a CSP's Cloud Service Offering (recognizing that a CSP may have multiple offerings).
- Entities such as program managers within the DoD Components responsible for instantiating information systems and applications leveraging a CSP's Cloud Service Offering are referred to as Mission Owners.

1.1 Purpose and Audience

The Federal Risk and Authorization Management Program (FedRAMP) is a Federal Government program focused on enabling secure cloud computing for the Federal Government. DOD, by the virtue of its warfighting mission, has unique information protection requirements that extend beyond the controls assessed via FedRAMP. This document outlines the controls and additional requirements necessary for using cloud-based solutions within the DOD.

The Cloud Computing SRG serves several purposes:

- Provides security requirements and guidance to non-DoD owned and operated Cloud Service Providers (CSPs) that wish to have their service offerings included in the DoD Cloud Service Catalog.
- Establishes a basis on which DoD will assess the security posture of a CSP's service offering; supporting the decision to grant a DOD Provisional Authorization to Operate (P-ATO) that allows a CSP to host DoD missions.
- Defines the policies, requirements, and architectures for the use and implementation of commercial cloud services by DoD Mission Owners.
- Provides guidance to DOD Mission Owners and Assessment and Authorization officials (formerly Certification and Accreditation) in planning and authorizing the use of a CSP.

The audience for this Cloud Computing SRG includes:

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

1.2 Authority

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

DoDI 8500.01, entitled Cybersecurity, directs Director DISA, under the authority, direction, and control of the DoD CIO to develop and maintain Control Correlation Identifiers (CCIs), Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible.

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

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

1.3 Scope and Applicability

This Cloud Computing SRG establishes the DoD security objectives to host DoD missions up to and including SECRET on CSOs. Missions above SECRET must follow existing applicable DoD policies and are not covered by this Cloud Computing SRG.

This SRG applies to DoD owned and operated and non-DoD owned and operated Cloud Service Providers, (CSPs) whether they are commercial or non-DoD Federal Government organizations. This SRG also applies to any supporting cloud services provider or facilities provider that the CSP might leverage to provide a complete service. While the CSP's overall service offering may

be inheriting controls and compliance from a third party, the prime CSP is ultimately responsible for complete compliance.

While DoD enterprise service programs providing cloud capabilities or service offerings (e.g. milCloud, Defense Enterprise Email) are subject to these same requirements, compliance with many of the requirements will be inherited from the facilities in which they are housed and other DoD protection capabilities. However, the process for authorizing government provided services is based on using DOD's assessment and authorization process under the DoD Risk Management Framework (RMF); as opposed to using the FedRAMP and FedRAMP+ assessment processes outlined in this document for non-DoD offerings.

This SRG establishes the DoD security requirements for DoD Mission Owners when contracting for and using Software as a Service (SaaS) offerings, and when implementing their systems and applications on 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 SRG considers IaaS and PaaS as being closely 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.

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

Security Requirements Guides (SRGs) are collections of requirements applicable to a given technology family, product category, or an organization in general. The security requirements contained within SRGs, 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. SRGs provide non-product specific requirements to reduce the security vulnerabilities of systems and applications.

While the SRGs define the high level requirements for various technology families and organizations, the Security Technical Implementation Guides (STIGs) are the detailed guidelines for specific products. In other words, STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product's technology area.

The security requirements contained within 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. 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 results in a given system being subject to multiple SRGs and/or STIGs.

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

1.5 SRG and STIG Distribution

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

1.6 Document Revisions and Update Cycle

SRGs and STIGs may be revised and updated to accommodate policy changes, new or changed requirements, new threats and mitigations, a package reorganization, and to correct errors or to provide clarity on any given topic. Such updates are typically published as a dot release of a major version. DISA FSO maintains a quarterly release cycle for these updates. The release schedule can be found at <http://iase.disa.mil/stigs/Pages/fso-schedule.aspx>.

Major updates to a SRG or STIG result in a version change rather than a dot 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.

Comments or proposed revisions to this document should be sent via email to disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA FSO quarterly maintenance release schedule.

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. Sections 5-6 outline specific security requirements to be addressed in authorizing and operating cloud capabilities.

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 – Risk Assessment of Cloud Service Offerings: Provides an overview of the assessment and authorization processes used for granting a DOD provisional authorization (P-ATO), and explains how a P-ATO can be leveraged by a Mission Owner and its Authorizing Official (AO) in support of an Authority to Operate (ATO) decision.

Section 4 – Impact Levels and Security Objectives: Explains the concept of “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 5 – Security Requirements: Details the requirements associated with enabling CSP capabilities. This includes specific Information Assurance (IA) control requirements (FedRAMP and DOD specific); Continuous Monitoring requirements; identification and authentication; SRG/STIG compliance; connectivity architecture and requirements/constraints; location/jurisdiction; separation requirements; and other specific requirements.

Section 6 – Computer Network 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.

DRAFT

2 BACKGROUND

2.1 Cloud Computing, Cloud Service, and Cloud Deployment Models

The National Institute of Standards and Technology (NIST) provides definitions for cloud computing, cloud service models and cloud deployment models in Special Publication (SP) 800-145¹. This Cloud Computing SRG is written in accordance with and leverages these definitions.

According to NIST, 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.

Cloud service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The components offered in IaaS form the basis for PaaS, while the components offered in PaaS form the basis of SaaS. Service offerings that provide data storage without compute services will be considered as a subset of IaaS. While vendors may market and name their offerings as they wish, the Broker will categorize them into one of the three NIST models.

Cloud deployment models include Public, Private, Community, and Hybrid. Please see NIST SP 800-145 for the detailed definitions of these models.

Note that cloud computing and cloud services, as used in this SRG, does not refer to classic forms of computing and applications where hardware (whether it is virtualized or not) is typically employed or built by organizations for their own use. A service offering from a provider organization to a single or organizational customer must be part of the construct.

2.2 Cloud Service Provider (CSP)

A Cloud Service Provider (CSP) is an entity that offers one or more cloud service types in one or more deployment models (as defined by NIST) to users within the same organization or customers in other government or non-government/commercial organizations. A CSP might leverage or outsource services of other organizations and other CSPs; such as placing certain servers or equipment in third party facilities such as data centers, carrier hotels / collocation facilities, and Internet Network Access Points (NAPs). When it comes to SaaS, the CSP offering the service may actually leverage one or more third party CSP's IaaS or PaaS service offerings to build their service. Caution must be exercised when selecting a CSP to understand if they are leveraging third party facilities or cloud services.

2.3 DoD Risk Management Framework (DoD RMF)

DoDI 8510.01 defines the DoD RMF which is based on the concepts of the Federal RMF defined in various NIST special publications along with the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253. The NIST Special publications implemented by these policies include, but are not limited to, SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems* and SP 800-53, *Security and Privacy Controls for Federal*

¹ NIST SP 800-145: <http://csrc.nist.gov/publications/PubsSPs.html>

Information Systems and Organizations. The full set of NIST documents can be found at <http://csrc.nist.gov/publications/PubsSPs.html>.

2.4 Federal Risk and Authorization Management Program (FedRAMP)

The Federal Risk and Authorization Management Program (FedRAMP) is a Federal Government program focused on enabling secure cloud computing for the Federal Government. FedRAMP implements the Federal Government RMF as defined in NIST special publications for cloud computing in the Federal Government.

FedRAMP is mandated for use by all Federal Agencies by the Office of Management and Budget (OMB) as their systems and applications are migrated to the commercial cloud under the Federal Government's Cloud-First initiatives. OMB policy requires Federal departments and agencies using commercial cloud services to use FedRAMP approved CSPs by June 2014 and share Agency Authority to Operate (ATO)s with the FedRAMP Secure Repository.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. 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 Provisional Authorization (PA) to host Federal Government missions.

DoD leverages FedRAMP PAs and U.S. Government Federal Agency ATO packages residing in the FedRAMP Secure Repository, including all supporting documentation, as part of the DoD security assessment process.

3 RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS

The shift to cloud computing necessitates changes in the Risk Management processes. The goal is to manage security requirements and controls, relative to the criticality of the data, in a cost effective and efficient manner, while assuring the security of DoD's core network. DOD has defined impact levels (discussed in section 4, "IMPACT LEVELS / SECURITY OBJECTIVES") that align to the criticality and sensitivity of data. Therefore, the impact level at which a CSP's Cloud Service Offering (CSO) is provisionally authorized is critical in determining the appropriate CSP(s) to support a mission.

3.1 Assessment of Commercial/Non-DoD Cloud Services

Security Requirements for DOD cloud computing extend beyond the controls assessed as part of the FedRAMP LOW or FedRAMP MODERATE baselines. DOD requirements are viewed as a combination of the controls in the FedRAMP MODERATE baseline and the DOD specific controls/requirements outlined in this SRG (referred to as FedRAMP+). Where possible, DoD leverages documentation and artifacts in the FedRAMP Secure Repository and additional CSP proprietary artifacts. FedRAMP+ requirements will be assessed by a FedRAMP certified 3PAO or an approved DoD assessor. The DoD promotes the use of parallel activities (FedRAMP and FedRAMP+) to minimize cost and create efficiencies in the assessment process. An overall assessment of risk is prepared to support a DoD P-ATO decision and listing in the DoD Cloud Service Catalog², available to DoD personnel. The DISA Authorizing Official (AO) (formerly the DISA DAA) approves DoD P-ATOs.

There are three paths that can be followed in assessing a CSP for a DoD P-ATO. 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 controls and requirements not addressed by FedRAMP.
- **FedRAMP Agency ATO:** CSPs having a Federal agency authorization based upon controls assessed by a certified 3PAO can be assessed for a DOD P-ATO provided that the authorization is accepted and listed in the FedRAMP agency authorizations. The information from the agency ATO will be supplemented with an assessment of the DoD-specific controls and requirements not addressed by FedRAMP.
- **DoD Self-Assessed P-ATO:** CSP is assessed by DoD assessment teams independent of FedRAMP. This is used for dedicated cloud service offering instantiations supporting the DoD or a private cloud offering. In this scenario, the CSP's assessment package will not be in the FedRAMP secure repository since private clouds are ineligible for inclusion in the FedRAMP catalog. When a FedRAMP authorization does not exist for a commercial CSP, the DoD organization with a need for the authorization will be required to support resourcing for the full assessment, in coordination with the Broker assessment team. This assessment of both the FedRAMP and FedRAMP+ requirements determines whether to grant a DoD P-ATO.

² <https://disa.deps.mil/disa/org/atb/Cloud%20Broker/Lists/Catalog/CatalogPageView.aspx>

3.2 Assessment of DoD Provided Cloud Services

DoD operated CSOs (e.g., milCloud) are subject to the same requirements found in this SRG and the same IA controls as commercial CSPs. However DoD CSP programs and services must follow DoD Risk Management procedures (DIACAP or DoD RMF) in accordance with DoDI 8510.01. DoD enterprise service programs that may be considered as a cloud service under the SaaS model (e.g., Defense Enterprise Email (DEE), Defense Connect Online (DCO), DoD Enterprise Portal Service (DEPS)), are also subject to the DODI 8510.01 requirements. Such programs are not subject to being assessed through FedRAMP and do not share DoD ATOs with the FedRAMP secure repository.

DoD is transitioning to the DoD RMF from the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP). DIACAP is based on a set of DoD specific IA controls; not the NIST 800-53 IA control catalog. Cloud services initiated and authorized under the DIACAP will be assessed and authorized using the RMF in accordance with DoD transition guidance.

3.3 Cloud Service Offering Risk Management

Risk management for the use of Cloud Service Offerings (CSO) by DoD must consider both the CSO and the supported mission (i.e., the CSP's customer's or Mission Owner's system or application). Each CSO must be granted a DOD P-ATO in order to host DOD mission systems. The P-ATO can 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). Additionally, there may be many controls that are "shared controls" where both the CSO and the Mission Owner need to address a requirement. The responsible AO leverages the P-ATO information, supplemented with an assessment of the risks within the Mission Owner's responsibility, in granting any form of an approval to operate.

This distinction is critical to understanding the DoD cloud security model as defined in this SRG.

3.3.1 Cloud Service Offering (CSO) Risk

The P-ATO provides a risk acceptance determination for the CSO against the appropriate DoD security requirements. It's important to recognize that the DoD certification and DoD P-ATO process determines CSO risk only. Overall mission risk will continue to be assessed and authorized by the Mission Owner's AO through the current DoD risk management process.

3.3.2 Mission Risk

The mission referred to here is the Mission Owner's purpose for which the CSO is being used. This may be the direct use of a SaaS CSO in the fulfillment of the mission or the instantiation of a mission system or application on an IaaS/PaaS CSO.

A Mission Owner will select an appropriate CSO from the DoD Cloud Service Catalog to support its mission system/application use-case based on its categorization via DoD 8510.01 defined processes. That CSO will have minimally been certified and provisionally authorized for use by the DISA AO, or may have a full ATO that might be applicable to the Mission Owner's needs. The Mission Owner must then subject their system/application/use-case through the required DoD risk management process to receive an Authority To Operate (ATO) from their assigned AO. The benefit of starting with a provisionally authorized CSO is that compliance

with many of the controls/enhancements is inheritable, to an extent, by the system/application/use-case. Mission Owners and their AOs must review the DoD P-ATO to be cognizant of the residual risk inherited from the CSO as they assess the mission system/application/use-case for its ATO.

3.3.3 Mission System Inheritance

The Mission Owner inherits compliance with the IA controls met by the CSO for the portion of the IA control that the CSP and CSO can meet. A Mission Owner's system or application built on an IaaS or PaaS offering will be subject to meeting many of the same IA controls within the system/application that the CSO must meet. On the other hand, Mission Owners contracting for SaaS offerings inherit the bulk of compliance with the IA controls from the CSO. Figure 1, illustrates this concept.

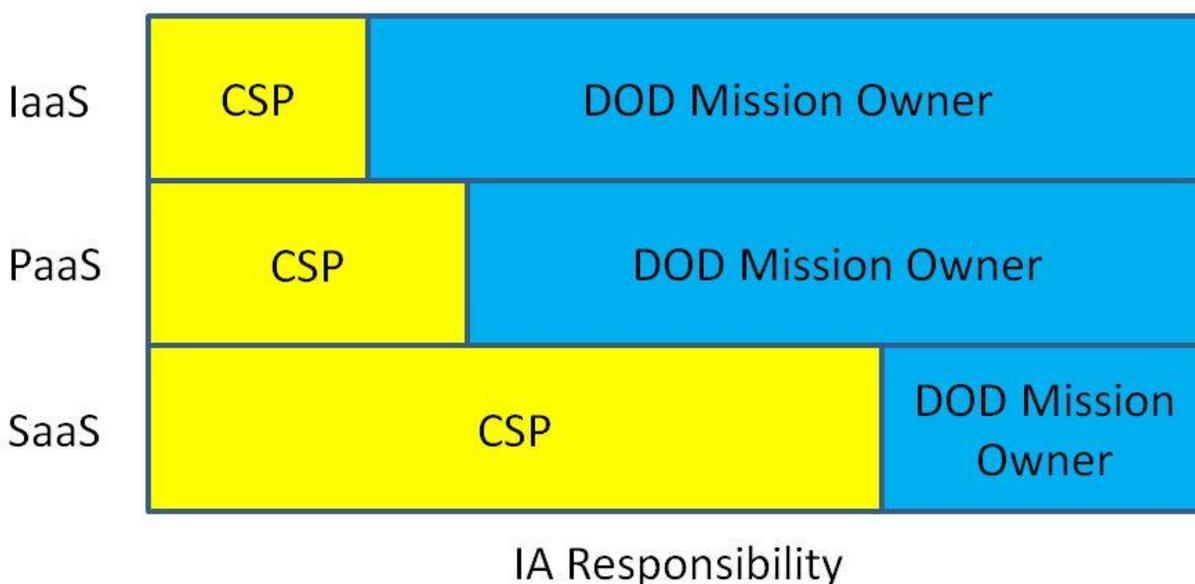


Figure 1 – Notional Division of Security Inheritance and Risk

3.4 CSP Transition from CSM v2.1 to Cloud Computing SRG v1r1

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

- Any new assessment starting after June 1, 2014 will immediately transition to FedRAMP v2 baselines based on NIST 800-53 rev4.
- CSPs currently in the process of being assessed against FedRAMP v1 baselines based on NIST 800-53 rev3 on June 1, 2013 will continue on this track, but must transition to the FedRAMP v2 baselines by their next annual reauthorization.
- CSPs currently in continuous monitoring will have until their next annual reauthorization to complete the transition to FedRAMP v2 baselines.

Complete FedRAMP transition information may be found at <http://cloud.cio.gov/topics/fedramp-800-53-rev-4-guidance-cloud-service-providers-0>

The requirements in this SRG become effective immediately upon final publication for Mission Owners as do SRG and STIG requirements for all of DoD. However, the DoD migration plan for CSP assessments will mirror the FedRAMP plan as follows:

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

NOTE: CSP's wishing to transition sooner than later may do so at any time.

DRAFT

4 IMPACT LEVELS / SECURITY OBJECTIVES

Cloud security impact levels are defined by the combination of information to be stored and processed in the CSP infrastructure / service offerings and the potential impact should the confidentiality or the integrity of the information be compromised. There are many combinations of information type and potential impact. DoD Mission Owners are expected to categorize their mission system/data/application in accordance with DoDI 8510.01 and CNSSI 1253; then use the impact level that most closely aligns to the required baselines. Impact levels, including changes from previous versions of the Cloud Security Model, are described further below.

4.1 Impact Levels

The previously published Cloud Security Model defined 6 Impact Levels. In order to simplify the impact level selection process, the number of Impact Levels was reduced from 6 to 4. This was accomplished by deprecating Impact Levels 1 (public information) and 3 (low impact Controlled Unclassified Information (CUI) and including these information types in the next higher impact level. The numeric designators for the Impact Levels have not changed to remain consistent with previous versions of the Cloud Security Model; leaving Impact Levels 2, 4, 5, and 6.

Additionally, the security control baseline for all levels has been changed to moderate as defined by CNSSI 1253. This modification from high confidentiality and high integrity is intended to better align with the categorization of most DoD customer systems that will be deployed to cloud service offerings.

Impact Level 6 is described in this Cloud Computing SRG. It requires a similar set of tailored controls as Level 5, and includes the CNSSI-1253 Appendix F, Attachment 5 Classified Information Overlay controls.

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

4.1.1 Level 1; Unclassified Information approved for Public release:

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

4.1.2 Level 2; Non-Controlled Unclassified Information:

Includes all data cleared for public release as well as unclassified information not designated as CUI but which requires some level of access control.

4.1.3 Level 3; Controlled Unclassified Information:

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

4.1.4 Level 4; Controlled Unclassified Information:

Level 4 accommodates CUI which is the categorical designation that refers to unclassified information that under law or policy requires protection from unauthorized disclosure as established by Executive Order 13556 (November 2010). Designating information as CUI is the

responsibility of the owning organization. Determination of the appropriate impact level for a specific mission with CUI data will be the responsibility of the mission AO.

CUI contains a number of categories³, including, but not limited to the following:

- Export Control³--Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. This includes dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
- Privacy Information³--Refers to personal information, or, in some cases, *personally identifiable information*, (PII)⁴ as defined in Office of Management and Budget (OMB) M-07-16⁵, or *means of identification* as defined in 18 USC 1028(d)(7).
- Protected Health Information (PHI)⁶ as defined in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).
- Other information requiring explicit CUI designation (i.e. For Official Use Only, Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information).

4.1.5 Level 5; Controlled Unclassified Information:

Level 5 accommodates CUI that requires a higher level of protection as deemed necessary by the information owner, public law, or other government regulations. Level 5 accommodates unclassified National Security Systems (NSSs).

4.1.6 Level 6; Classified Information up to SECRET:

Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD). At this time, only the potential for classified information up to the level of SECRET, in accordance with the applicable executive orders, is being considered. Services running at higher classification levels, to include compartmented information, are governed by other policies and are beyond the scope of this document.

NOTE: All levels can host data/information from a lower level.

³ <http://www.archives.gov/cui/registry/category-list.html>

⁴ <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

⁵ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>

⁶ <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/>

4.2 Security Objectives (Confidentiality, Integrity, Availability)

Impact Levels consider the potential impact should the confidentiality or the integrity of the information be compromised. The construct does not address the impact of availability because it is expected that the Mission Owner will include its availability requirements in the contract or a service level agreement with the CSP. However, all CSPs will be evaluated to determine the maximum level of availability they offer. This evaluation does not prevent a CSP from being included in the DoD Cloud Service Catalog; it is only used to facilitate the matching of a DoD customer to one or more appropriate cloud services meeting their needs. Note that the Mission Owner must ensure that the SLA with the CSP is specific and inclusive for the required availability. For example, if the requirement is “CSP maintenance affecting system availability must be coordinated 4 weeks in advance and only conducted between 02:00 and 04:00 EST on Sunday morning”, then the SLA should detail the requirement. Recommended SLA availability controls are provided under the FedRAMP+ Controls/Enhancements in Section 5.1.5, *Controls/Enhancements to be Addressed in the Contract/SLA*.

According to Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 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]. 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.

The security model includes the FIPS-199 defined three levels to designate the impact of a loss of confidentiality or a loss of integrity. These are defined in Table 1.

Table 1 - Potential Impact Definitions for Security Objectives

Security Objective	Potential Impact		
	Low	Moderate	High
<i>Confidentiality</i>	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.
<i>Integrity</i>	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.

The security control baseline for all Impact Levels is based on moderate confidentiality and moderate integrity. If a Mission Owner has higher potential impacts, specific requirements to address/mitigate this risk must be included as part of the contract/SLA.

5 SECURITY REQUIREMENTS

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

- Security requirements for assessing commercial and DoD CSPs for inclusion in the DoD cloud service catalog.
- Security requirements for CSP's service offerings.
- Security requirements for Mission Owner's systems/applications instantiated on IaaS/PaaS.

5.1 DoD Policy Regarding Security Controls

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

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

See NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*,⁷ for a definition of NSS and further information.

5.1.1 DoD use of FedRAMP Security Controls

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

DoD is using the FedRAMP v2 Moderate baseline which when supplemented with DoD Cs/CEs is used to assess CSPs toward awarding a DoD provisional authorization at all information impact levels.

5.1.2 DoD FedRAMP+ Controls/Enhancements

A tailored baseline of security Cs/CEs has been developed for each impact level for DoD. These baselines incorporate, but are not limited to, the FedRAMP Moderate baseline. The DoD cloud baseline Cs/CEs, which are beyond what is required by FedRAMP (otherwise referred to as FedRAMP+ Cs/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.

The CNSSI 1253 baseline used in support of DoD P-ATOs is based on Moderate Confidentiality and Moderate Integrity, not including a baseline for Availability (M-M-x). Availability is to 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+ controls/enhancements for each level. The FedRAMP Moderate Baseline includes approximately thirty two (32) Cs/CEs that are also contained in the CNSSI 1253 M-M-x baseline. Eighty eight

⁷ NIST SP 800-59: <http://csrc.nist.gov/publications/PubsSPs.html>

(88) of these Cs/CEs are not in the FedRAMP baseline. These were analyzed for their benefit and projected cost and approximately half were selected for the DoD cloud baselines. One control was selected at all levels (AC-23). The number of control enhancements selected varies by impact level.

Although the control baselines for all levels are based on those from CNSSI 1253, only impact Level 5 and 6 are designed to accommodate NSS. NSS-specific controls/enhancements have been included at these levels along with those required for the higher impact. This, however, does not preclude an unclassified non-NSS from operating at Level 5 if the mission requires the added security. Since Impact Level 6 is for classified NSS, it is also subject to the CNSSI 1253 Classified Overlay which imposes ninety eight (98) additional controls/enhancements. For IaaS/PaaS service offerings, there may only be a portion of the classified overlay applicable to the CSP with the balance of the controls/enhancements 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.

Additionally, any level that deals with PII or PHI is additionally subject to the CNSSI 1253 Privacy Overlay (when published). This overlay adds most of the Privacy specific Cs/CEs from NIST SP 800-53 rev4 Appendix J Privacy Control Catalog and provides additional supplemental guidance for many of the selected Cs/CEs in all other families. It was developed in accordance with Privacy Act and HIPAA requirements leveraging experts and lawyers in both fields. Legal references are included as the basis for C/CE selection and supplemental guidance. This overlay is fully applicable to CSP's SaaS offerings that handle PII/PHI with some Cs/CEs (e.g., the required system of records notice in accordance with TR-2) being addressed by the Mission Owner. For IaaS/PaaS offerings, only a portion of the overlay may be applicable to the CSP with most Cs/CEs being fulfilled by the Mission Owner. This in no way alleviates any requirement incumbent upon the CSP for protecting privacy act information related to its customers and their accounts.

One of the goals for improving efficiency of Cloud Broker program is to accept the FedRAMP Provisional Authorization as the basis for granting a DOD P-ATO for Impact Level 2. After reviewing the controls required by CNSSI 1253, DOD has identified thirty six (36) FedRAMP+ Cs/CEs that warrant consideration for inclusion in the FedRAMP Moderate baseline; based on the value/assurances they provide for the entire Federal community.

The twenty five (25) FedRAMP+ Cs/CEs currently required for Impact Level 2 are part of the thirty six (36) identified for inclusion into the FedRAMP baseline. In the interim, the DISA AO is considering accepting the risk resulting from these not being assessed by DoD or FedRAMP for Impact Level 2 only. The residual risk from these controls would be documented; along with any supplemental information provided by the CSP or 3PAO regarding these controls.

*A Mission Owner AO may choose to require a CSP to meet the FedRAMP+ Cs/CEs listed in **Error! Not a valid bookmark self-reference.** under Level 2 by requiring them to be included in the contract or SLA.*

The risk acceptance of the twenty five (25) FedRAMP+ Cs/CEs would only apply for Impact Level 2; it does not apply to the other levels (e.g. 4/5/6 in which these Cs/CEs are listed.

[NOTE: Input regarding the above is encouraged from both industry and the DoD community.]

Table 2 provides a listing of the FedRAMP+ Cs/CEs applicable to each information impact level which includes only one additional base control. The rest are control enhancements. This does not include controls added by the Classified Information or Privacy overlays. These controls and control enhancements must be implemented and documented by the CSP. Assessment is discussed below. CSPs may offer equivalent controls or mitigations for consideration.

5.1.3 Risk Acceptance for FedRAMP+ Controls/Enhancements at Level 2

One of the goals for improving efficiency of Cloud Broker program is to accept the FedRAMP Provisional Authorization as the basis for granting a DOD P-ATO for Impact Level 2. After reviewing the controls required by CNSSI 1253, DOD has identified thirty six (36) FedRAMP+ Cs/CEs that warrant consideration for inclusion in the FedRAMP Moderate baseline; based on the value/assurances they provide for the entire Federal community.

The twenty five (25) FedRAMP+ Cs/CEs currently required for Impact Level 2 are part of the thirty six (36) identified for inclusion into the FedRAMP baseline. In the interim, the DISA AO is considering accepting the risk resulting from these not being assessed by DoD or FedRAMP for Impact Level 2 only. The residual risk from these controls would be documented; along with any supplemental information provided by the CSP or 3PAO regarding these controls.

*A Mission Owner AO may choose to require a CSP to meet the FedRAMP+ Cs/CEs listed in **Error! Not a valid bookmark self-reference.** under Level 2 by requiring them to be included in the contract or SLA.*

The risk acceptance of the twenty five (25) FedRAMP+ Cs/CEs would only apply for Impact Level 2; it does not apply to the other levels (e.g. 4/5/6 in which these Cs/CEs are listed).

[NOTE: Input regarding the above is encouraged from both industry and the DoD community.]

Table 2 - DoD FedRAMP+ IA Controls/Enhancements

SP 800-53r4 Cont./Enh. ID	Level 2	Level 4	Level 5	Level 6
AC-06 (07)	X	X	X	X
AC-06 (08)	X	X	X	X
AC-17 (06)	X	X	X	X
AC-18 (03)	X	X	X	X
AC-23	X	X	X	X
AT-03 (02)	X	X	X	X
AT-03 (04)	X	X	X	X
AU-04 (01)	X	X	X	X
AU-06 (04)		X	X	X

AU-06 (10)		X	X	X
AU-12 (01)		X	X	X
CA-03 (01)			X	n/a
CM-03 (04)		X	X	X
CM-03 (06)	X	X	X	X
CM-04 (01)	X	X	X	X
CM-05 (06)	X	X	X	X
IA-02 (09)	X	X	X	X
IA-05 (13)	X	X	X	X
IR-04 (03)	X	X	X	X
IR-04 (04)		X	X	X
IR-04 (06)	X	X	X	X
IR-04 (07)	X	X	X	X
IR-04 (08)	X	X	X	X
IR-06 (02)		X	X	X
MA-04 (03)		X	X	X
MA-04 (06)	X	X	X	X
PE-03 (01)		X	X	X
PL-08 (01)			X	X
PS-04 (01)			X	X
PS-06 (03)			X	X
SA-04 (07)			X	X
SC-07 (10)		X	X	X
SC-07 (11)			X	X
SC-07 (14)				X
SC-08 (02)			X	X
SC-23 (01)	X	X	X	X
SC-23 (03)	X	X	X	X

SC-23 (05)			X	X
SI-02 (06)	X	X	X	X
SI-03 (10)			X	X
SI-04 (12)	X	X	X	X
SI-04 (19)		X	X	X
SI-04 (20)	X	X	X	X
SI-04 (22)	X	X	X	X
SI-10 (03)	X	X	X	X
Total	25	35 PLUS Privacy Overlay if required	44 PLUS Privacy Overlay if required	44 PLUS 98 from Classified Overlay

NOTE: RE: Level 2 CSOs containing only publicly releasable information; CM-03 (06), IA-05 (13), SC-23 (01), and SC-23 (03) are applicable to both privileged and non-privileged users at Level 2. However, if the IS contains only publicly releasable information and is accessed by the general public without requiring a login, these CEs are only applicable to privileged users managing these ISs.

5.1.4 Parameter Values for Security Controls and Enhancements

Many NIST SP 800-53 Security Controls and enhancements contain parameter values that are left, by NIST, to the Organization to define. For those controls required by FedRAMP and the DoD, the parameter values are defined in Appendix D.

5.1.5 Controls/Enhancements to be Addressed in the Contract/SLA

Table 3 shows the Cs/CEs designated for the Mission Owner to address in the contract or SLA. While these Cs/CEs generally address system availability, they relate to the availability of information useful for continuous monitoring, incident response, and other security issues. It must be noted that this listing does not preclude the Mission Owner from addressing any control or enhancement from any CNSSI 1253 baseline or the NIST SP 800-53 rev4 in the contract/SLA if they need the control/enhancement to be provided/met by the CSP to secure their system or application.

Table 3 - IA Controls/Enhancements to be addressed in the contract/SLA

SP 800-53r4 Cont./Enh. ID	Level 2	Level 4	Level 5	Level 6

AC-02 (13)		X	X	X
AC-03 (04)	X	X	X	X
AC-12 (01)			X	X
AC-16	X	X	X	X
AC-16 (06)	X	X	X	X
AU-10			X	X
IA-03 (01)		X	X	X
PS-04 (01)		X		
PS-06 (03)		X		
SA-12			X	X
SA-19			X	X
SC-07 (11)		X		
SC-07 (14)		X	X	
SC-18 (03)			X	X
SC-18 (04)			X	X
Total	3	9	12	11

5.2 Legal Considerations

5.2.1 Jurisdiction/Location Requirements

Legal considerations, including legal jurisdiction, controls where DoD and US government data can be located. All data /information stored and processed for the DoD must reside in a facility under the legal jurisdiction of the US or as defined in a treaty or special agreement between the US and another jurisdiction. CSPs will maintain all government data that is not physically located on DoD premises within the 50 States, the District of Columbia, and outlying areas of the US. Outlying areas include US territories and US government operated and controlled facilities located on foreign soil such as an embassy or DoD base, camp, post, or station (B/C/P/S). This restriction is applicable to all impact levels.

DoD CSPs will, and commercial CSPs may (under DoD contract), instantiate their cloud service architecture on DoD premises (DoD on-premises) which will directly connect to DoD networks. DoD on-premises includes DoD data centers, other facilities located on a DoD B/C/P/S, or in a commercial or another government facility (or portions thereof) under the direct control of DoD personnel and DoD security policies. A commercial facility in this sense means a building or space leased and controlled by DoD. Physical facilities may be permanent buildings or portable

structures such as transit/shipping containers. An example of the latter might be a container housing a commercial CSP's infrastructure located adjacent to a Core Data Center (CDC) and connected to its network as if it was inside the building. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time and update that list as new physical locations are added.

5.2.2 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 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.

Dedicated infrastructure, for the purpose of this SRG, refers to the physical cloud infrastructure supporting the virtualization technology being physically separate from any non-DoD or non-Federal Government tenants. This is also referred to as a private or community cloud. In this context, a private cloud refers to one limited to the DoD, while a community cloud refers to a cloud limited to the DoD and other Federal Government agencies.

Shared infrastructure, for the purpose of this discussion, refers to the physical cloud infrastructure being available to non-DoD and non-Federal Government tenants. This is also referred to as a public cloud.

It is important to note that while clouds marketed as "ITAR compliant", "government clouds", or "clouds for government" might restrict data location to US jurisdiction, they do not necessarily meet the standard for "dedicated" for the Federal Government or DoD. If the cloud service, or the underlying infrastructure it resides on, contains any non-Federal US government tenant such as state or local governments, industry partners, or foreign governments, it is a considered shared infrastructure for purposes of this SRG.

NOTE: The use of the term "ITAR compliant" in a CSP's marketing documentation may or may not mean that the Department of State's Directorate of Defense Trade Controls or the Department of Commerce's Bureau of Industry and Services certified and documented the service offering as truly ITAR compliant. The CSP or DoD Mission Owner must validate such claims before the Mission Owner considers the service offering based on its alleged compliance.

5.2.2.1 Impact Level 2 Location and Separation Requirements

Impact Level 2 cloud services can be offered on either shared or dedicated infrastructure. Information that can be processed and stored at Impact Level 2 can be processed 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." An "ITAR compliant" government community cloud, e.g., "gov" or "for gov" service offering might fulfill this requirement if validated as such.

5.2.2.2 Impact Levels 4 and 5 Location and Separation Requirements

Information that must be processed and stored at Impact Levels 4 and 5 can only be processed in a dedicated infrastructure; 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.” This excludes public and “ITAR compliant” government community cloud, e.g., “gov” or “for gov” service offerings. The following applies:

- Only DoD private or Federal Government community clouds are eligible for Impact Levels 4 and 5.
- Virtual separation between DoD and Federal Government tenants is permitted.
- Physical separation from non-DoD/non-Federal Government tenants is required.

5.2.2.3 Impact Level 6 Location and Separation Requirements

Impact Level 6 is reserved for the storage and processing of classified information. The following applies:

- Impact Level 6 information up to the SECRET level may be stored and processed in a dedicated cloud infrastructure located in facilities approved for the processing of classified information; rated at the highest level of classification of the information being stored and/or processed.
- On-premises locations are approved through DoD processes and are operated in accordance with DoD and Director of National Intelligence (DNI) policies.
- Off-premises locations that restrict the physical location of the information as described in section 5.2.1, “Jurisdiction/Location Requirements” are approved in accordance with the National Industrial Security Program (NISP) as defined in Executive Order 12829 and the National Industrial Security Program Operating Manual (NISPOM)⁸, DoD 5220.22-M
- A Facility Security Clearance⁹ and cleared personnel are required
- The hosting organization must operate the facility in accordance with the NISPOM.
- Virtual separation between DoD and Federal Government tenants is permitted.
- Non-DoD/non-Federal Government tenants are not permitted to use the same infrastructure.

5.3 Ongoing Assessment

Like FedRAMP, DoD requires an ongoing assessment and authorization capability for CSPs providing services to the DoD. This capability is built upon the foundation of the FedRAMP continuous monitoring strategy, as described in the FedRAMP CONOPS and Continuous Monitoring Strategy Guide.

5.3.1 Continuous Monitoring

CSPs, 3PAOs, and DoD assessors are responsible for providing deliverables attesting to the implementation of security controls. Continuous monitoring data flows will differ for CSPs depending on whether they have a FedRAMP JAB PA, a 3PAO assessed Federal Agency ATO, or DoD Self-Assessed P-ATO. These data flows are reflected in Figure 2, Figure 3, and Figure 4 respectively.

NOTE: DoD Self-Assessed means that the CSP has been assessed by DoD assessment teams.

⁸ NISPOM: <http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>

⁹ DSS Facility Clearance Branch: http://www.dss.mil/isp/fac_clear/fac_clear.html

In some cases, CSPs will provide continuous monitoring artifacts directly to the Broker. In such cases, the CSP will utilize commercial standard formats (e.g., comma-separated values, XML) that enable DoD to automate the ingest of continuous monitoring data.

5.3.1.1 CSPs in the FedRAMP Catalog

The FedRAMP catalog includes CSPs, acceptable to DoD, having a JAB PA or a 3PAO assessed Federal Agency ATO.

These CSPs will provide all reports required by the FedRAMP Continuous Monitoring Strategy Guide, including self- assessments, to the FedRAMP ISSO. The FedRAMP ISSO may request additional reports based on data collected. Continuous monitoring requirements for DoD are the same as those for FedRAMP, except that all reports and artifacts for FedRAMP+ Cs/CEs will be provided directly to the Broker. The DoD will review all artifacts provided through the FedRAMP continuous monitoring process in addition to artifacts regarding FedRAMP+ Cs/CEs on an ongoing basis to evaluate the CSO's risk posture.

The information will be used by Mission Owner AOs and the DISA AO to evaluate the risk posture of the complete system that is using the CSP's services. That evaluation will inform decisions to continue the ATO for the Mission Owner's system and the P-ATO for the CSP.

Figure 2 shows the normal flow of continuous monitoring information if the CSP has a FedRAMP JAB PA. In this case, the 3PAO should assess the FedRAMP+ Cs/CEs.

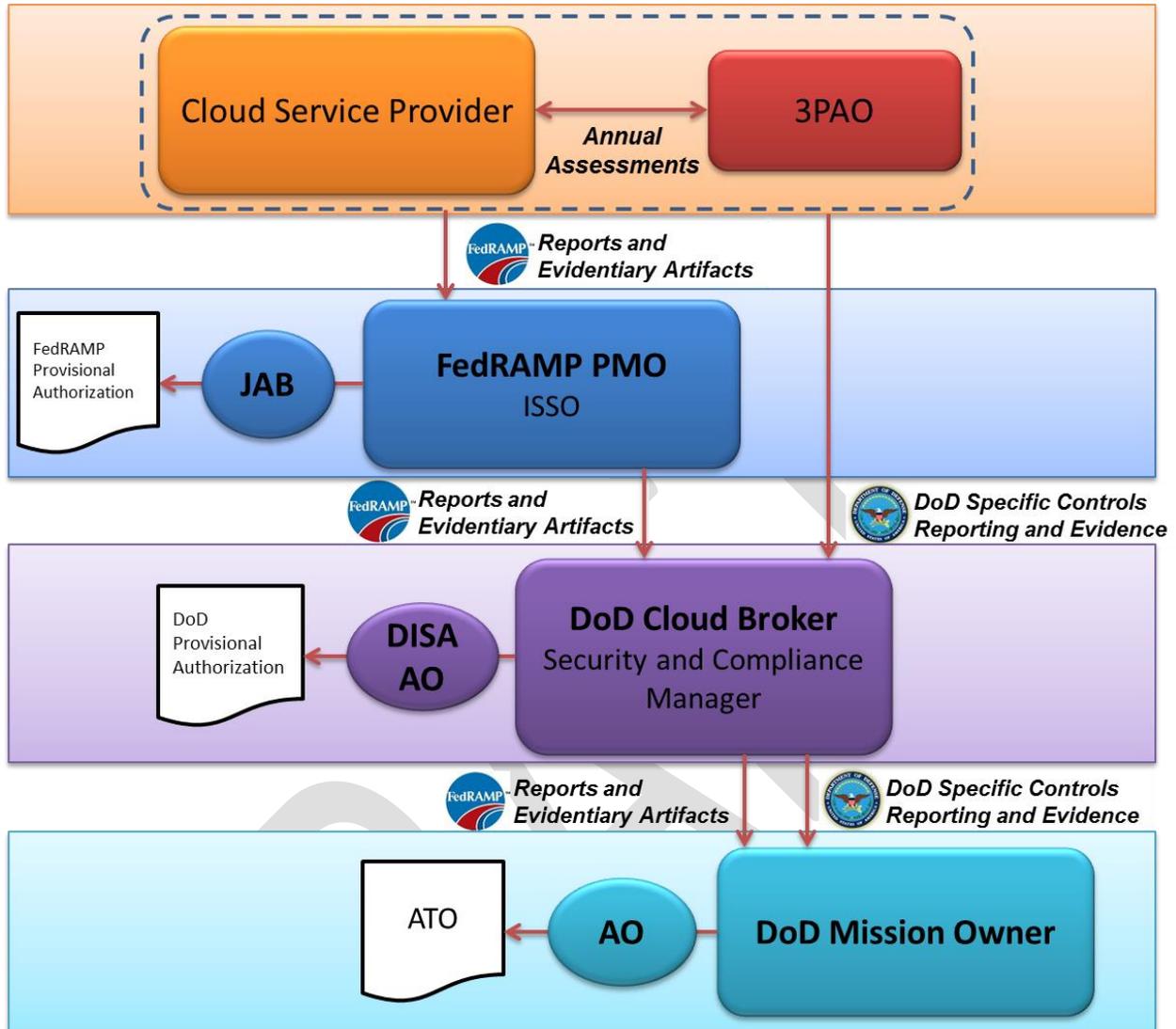


Figure 2 – DoD Continuous Monitoring for CSPs with a FedRAMP JAB PA

5.3.1.2 3PAO assessed Federal Agency ATO

Figure 3 shows the flow of continuous monitoring information if the CSP has a 3PAO assessed Federal Agency ATO listed in the FedRAMP catalog. When such a CSP also has a DoD P-ATO, DoD assesses the FedRAMP+ Cs/CEs.

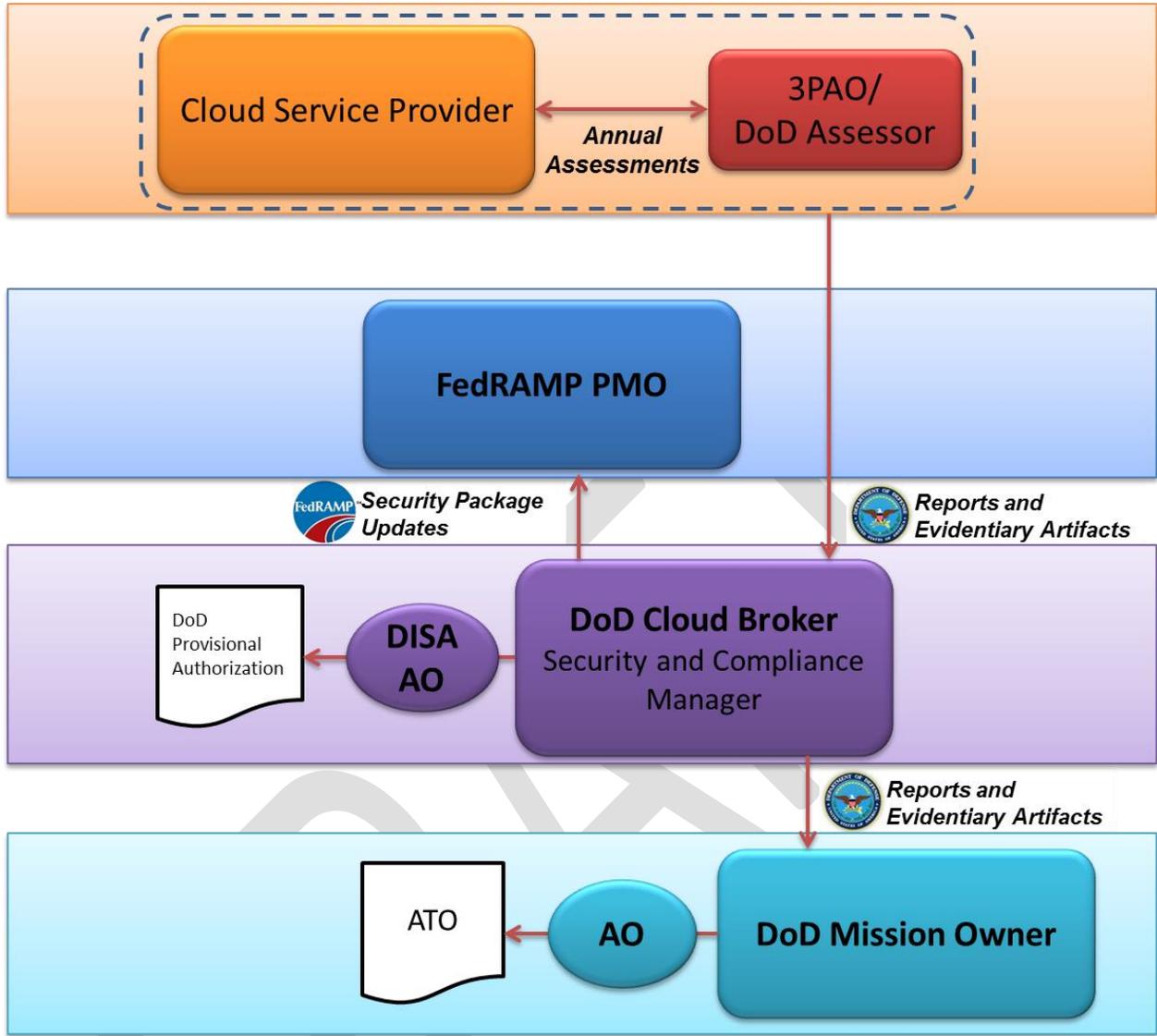


Figure 3 – DoD Continuous Monitoring for FedRAMP CSPs with a 3PAO assessed Federal Agency ATO

5.3.1.3 DoD Self-Assessed CSPs

Figure 4 shows the flow of continuous monitoring information for non-FedRAMP CSPs having a DoD P-ATO or ATO. Such CSPs will have been originally assessed by DoD assessors. 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 security plan. All reports and artifacts required by that continuous monitoring strategy will be provided by the CSP to the Broker. The Broker will, in turn, disseminate those artifacts to all mission owners utilizing that CSO, the DISA AO, and the Computer Network Defense Service Provider (CNDSP) entities as defined in section 6, “COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE.”

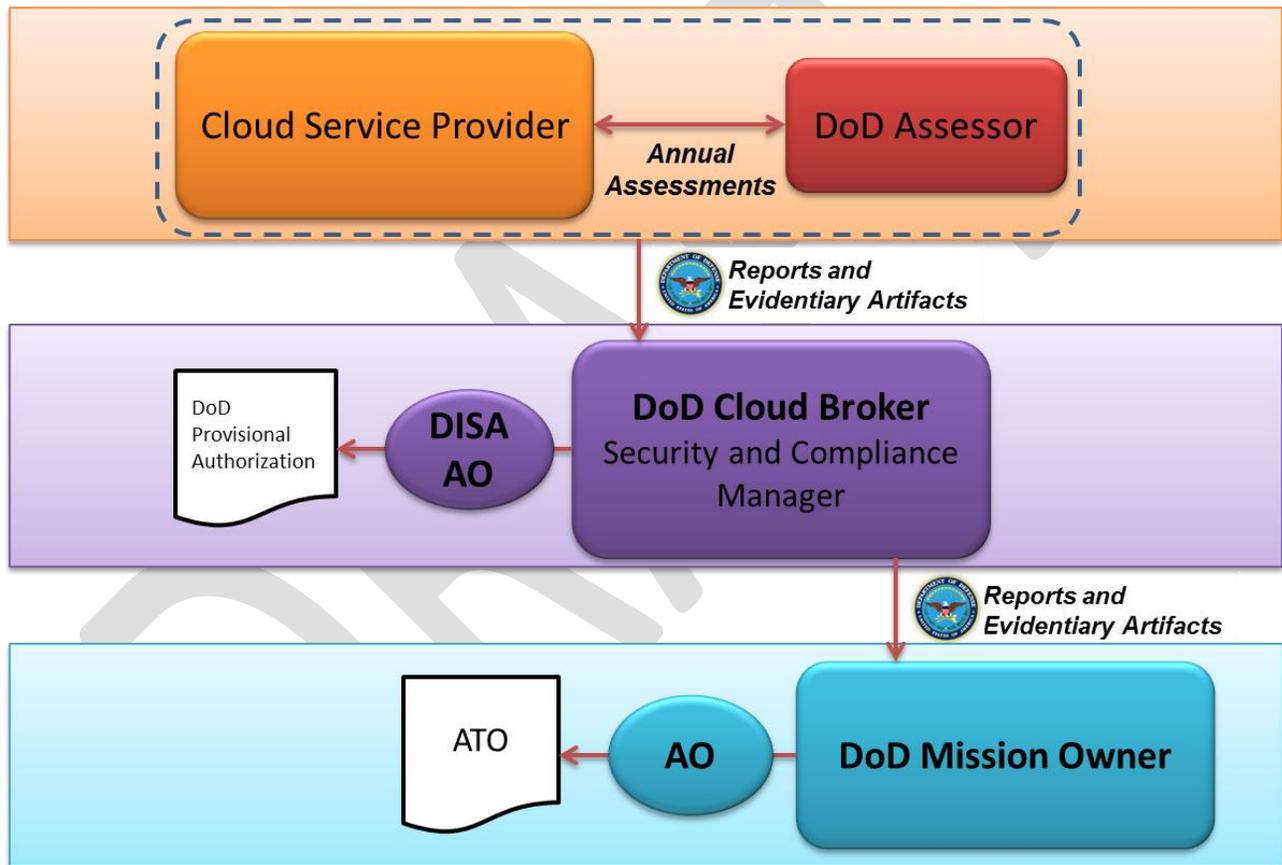


Figure 4 – DoD Continuous Monitoring for DoD Self-Assessed CSPs

5.3.2 Change Control

The DoD will review all significant changes planned by a CSP. Like 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 P-ATO or AO. Figure 5, Figure 6, and Figure 7 show these change control processes.

5.3.2.1 CSPs in the FedRAMP Catalog

FedRAMP 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 FedRAMP *Significant Change Security Impact Analysis Form* enumerates significant changes. The review of significant changes will be performed at multiple layers, as reflected in Figure 5. As part of the FedRAMP process, when the CSP holds a FedRAMP PA, they will notify the FedRAMP ISSO of any planned significant change and subsequently provide a Security Impact Analysis for the planned change. The planned change will be reviewed by the ISSO and then forwarded to the JAB for approval. During ISSO review, the DoD JAB Technical Representative (TR) will inform the FedRAMP ISSO if planned changes will adversely affect the security of the information hosted by the CSP for DoD cloud customers. The DoD JAB TR will notify the Broker, who will in turn notify all Mission Owners utilizing that CSO, the DISA AO, and the CNDSP entities as defined in section 6, “COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE.”

When a CSP is included in the FedRAMP catalog, but does not have a JAB PA, the CSP will notify the Broker directly, who will in turn notify the all Mission Owners utilizing that CSO, the DISA AO, and the CNDSP entities as defined in section 6, “COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE.” For CSPs in the DoD Cloud Service Catalog, the Security Impact Analysis must additionally cover the FedRAMP+ Cs/CEs. Once informed, the Broker will review the proposed change to ensure it will not adversely affect the security posture of the CSP with respect to the impact level at which it is authorized. The planned change will also be reviewed by the mission owners consuming the CSP’s services for any adverse impact with regard to their specific usage of the CSO. Any updates to the FedRAMP Security Package will be forwarded to the Broker.

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

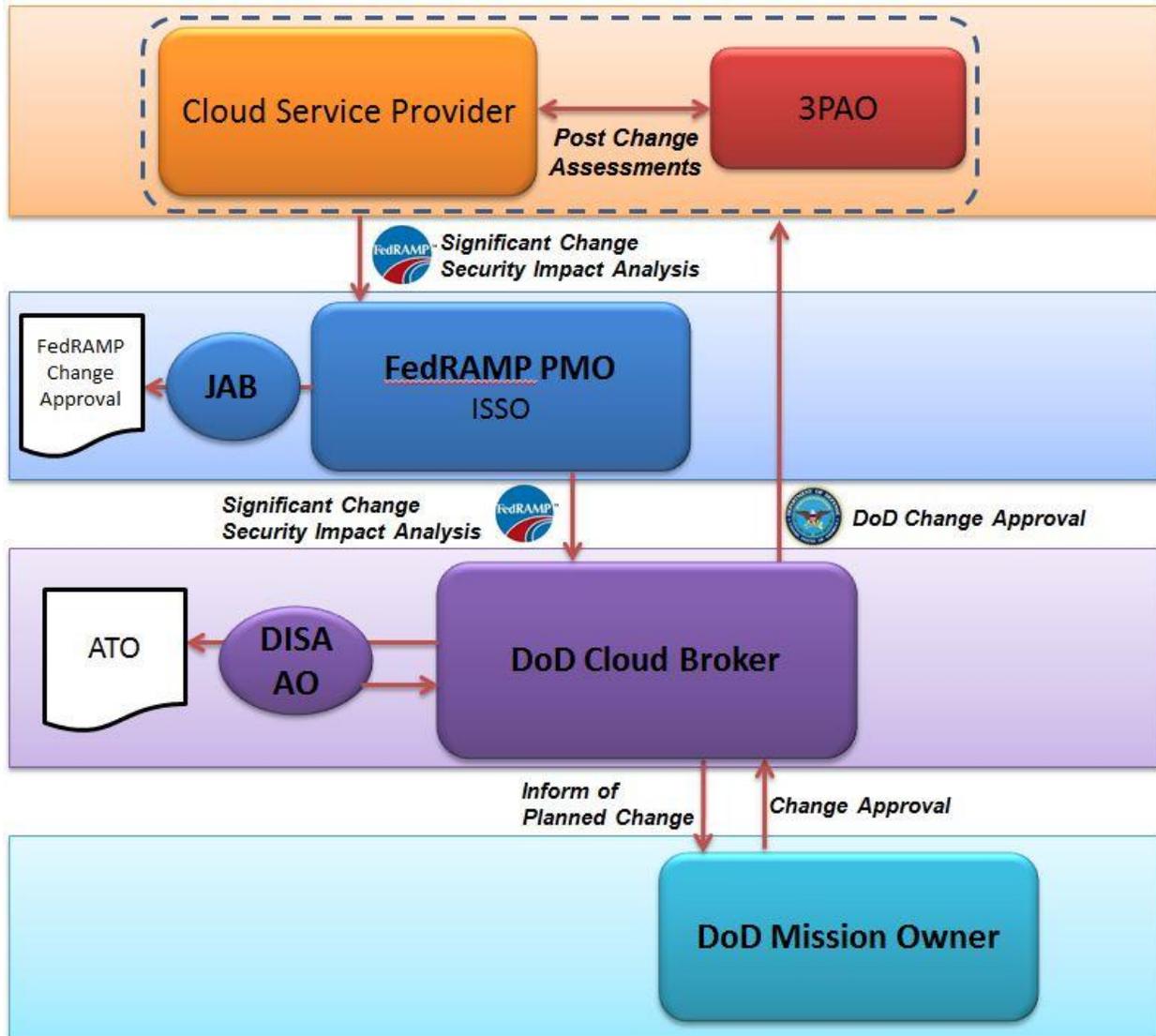


Figure 5 – DoD Change Control Process for CSPs with a FedRAMP JAB PA

5.3.2.2 3PAO assessed Federal Agency ATO

Figure 6 shows the normal flow of significant change information if the CSP has a 3PAO assessed Federal Agency ATO listed in the FedRAMP catalog. When such a CSP also has a DoD P-ATO, DoD assesses significant change information that may affect compliance with the FedRAMP+ Cs/CEs.

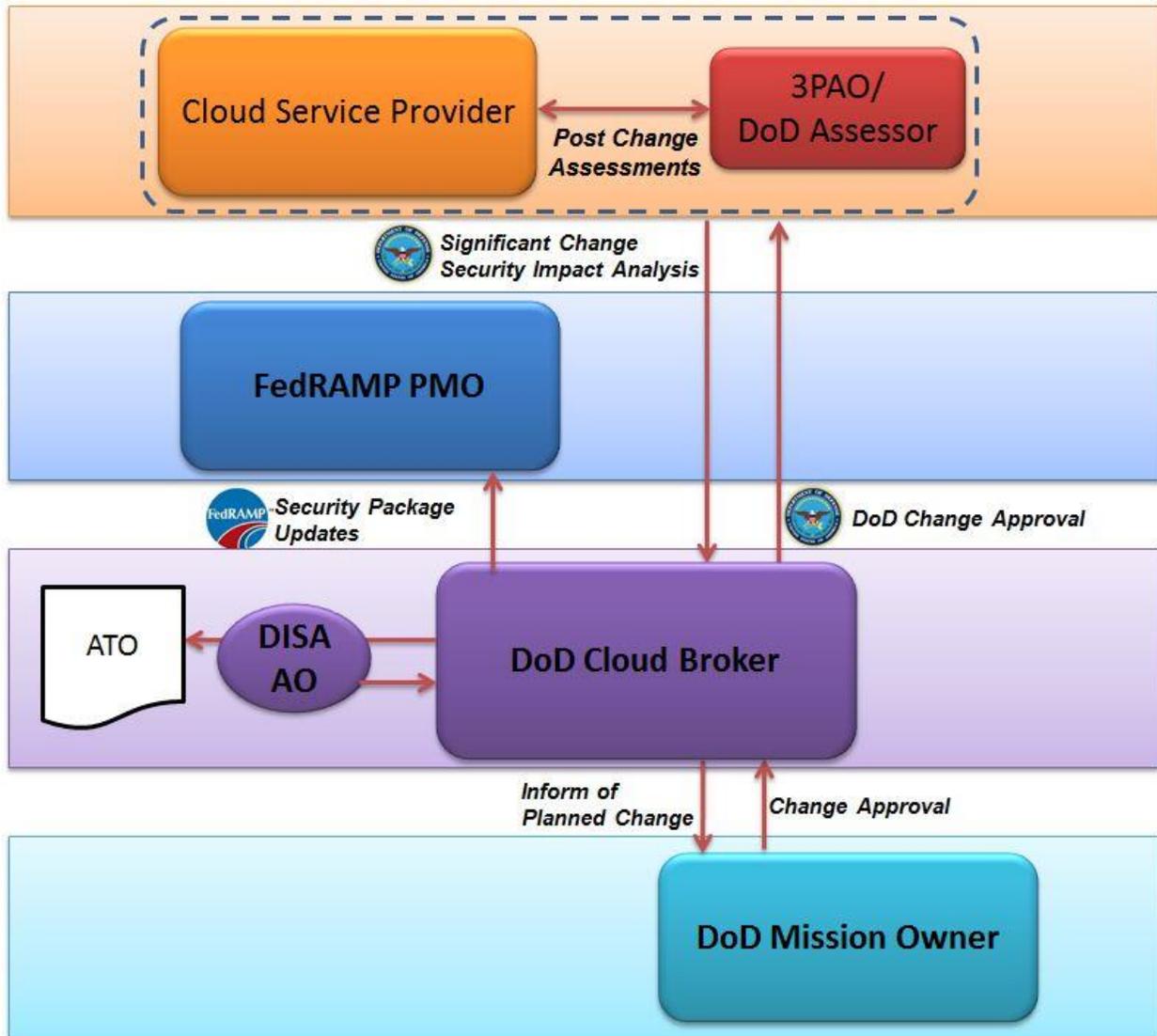


Figure 6 – DoD Change Control Process for FedRAMP CSPs with a 3PAO assessed Federal Agency ATO

5.3.2.3 DoD Self-Assessed CSPs

Figure 7 shows the flow of significant change for non-FedRAMP CSPs having a DoD P-ATO or ATO. Such CSPs will have been originally assessed by DoD assessors. 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 the Broker. The Broker will, in turn, disseminate those artifacts to all mission owners utilizing that CSO, the DISA AO, and the CNDSP entities as defined in section 6, “COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE.” These entities will review the proposed change to ensure it will not adversely affect the security posture of the CSP with respect its P-ATO or ATO. The planned change will also be reviewed by the mission owners consuming the CSP’s services for any adverse impact with regard to their specific usage of the CSO.

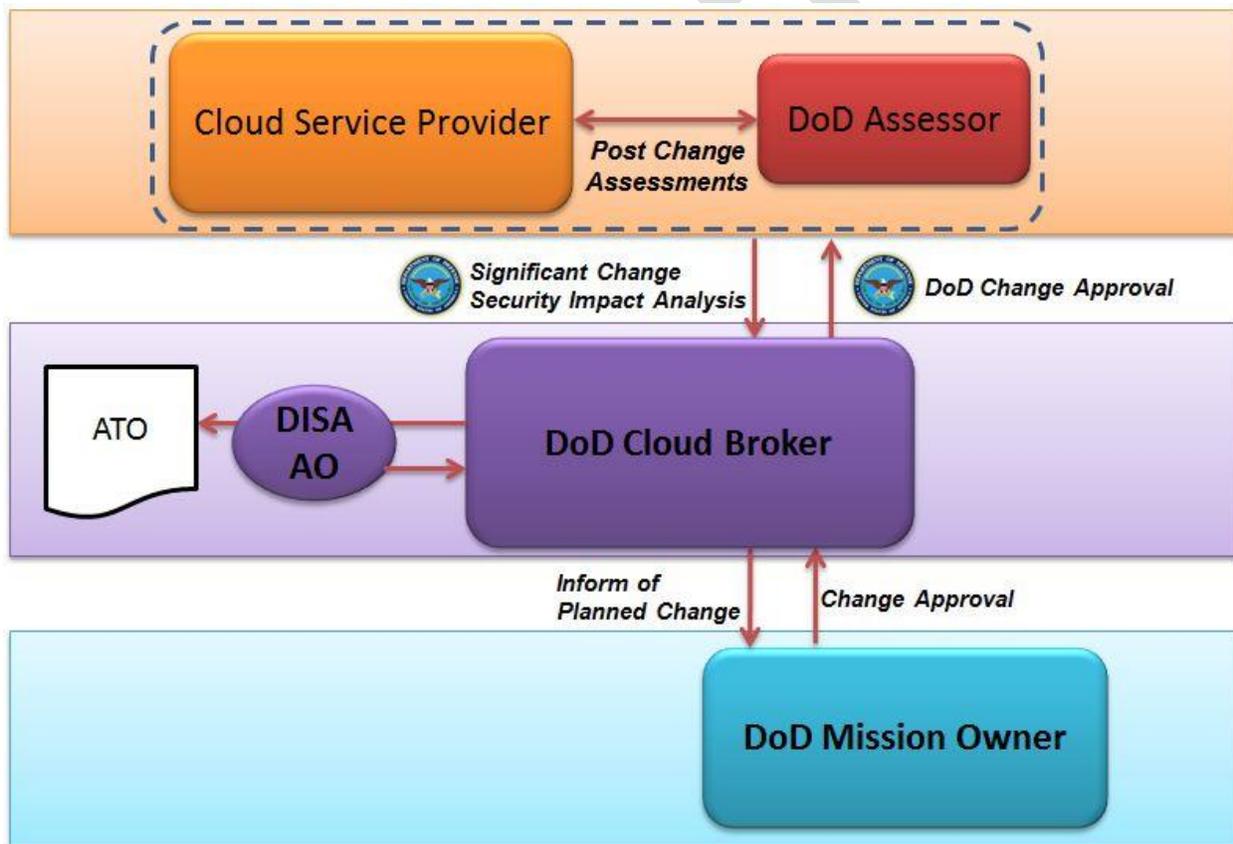


Figure 7 – DoD Change Control Process for DoD Self-Assessed CSPs

5.4 CSP use of DoD Public Key Infrastructure (PKI)

In accordance with (IAW) 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”, CSP’s are required to integrate with and use the DoD PKI for entity authentication. The following sections describe how the CSP fulfills its responsibilities:

- **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 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 Mission Owner’s 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, DoD Certificate Authorities, and follow DoD instructions and industry best practices for the management and protection of cryptographic keys.
- **Impact Levels 4 and 5:** Whenever a CSP is responsible for authentication of entities and/or identifying a hosted DoD information system, the CSP will use DoD PKI 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 Mission Owner’s privileged and non-privileged users. CSPs must make use of DoD OCSP or CRL resources for checking revocation of DoD certificates, DoD Certificate Authorities, and 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 a CSP is responsible for authentication of DoD entities and/or identifying a hosted DoD information system, the CSP will use DoD PKI in compliance with DoDI 8520.03 and CNSSP-25, and enforce the use of a physical token referred to as the CNSS SIPRNet Hardware Token for the authentication of 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, NSS Certificate Authorities, and 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.

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

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 a CSP responsibility
- Non-privileged Mission Owner access to CSP SaaS offerings
 - Integration with DoD PKI is a CSP responsibility
- Non-privileged user access to Mission Owners systems and applications instantiated on IaaS/PaaS.
 - Implementation is a Mission Owner responsibility.
- Mission Owner privileged user access to their systems and applications instantiated on IaaS/PaaS for the purpose of administration and maintenance.
 - Implementation is a Mission Owner responsibility.

Table 4 lists the Mission Owner credential types required at each impact level and the policy under which they are required.

Table 4 - Mission Owner Credentials

Impact Level	IAW DoD policy	IAW FedRAMP's selection of IA-2(12):
Level 2	<ul style="list-style-type: none"> ▪ 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 information minimally requires I&A through the use of a UID and password that meets DoD length and complexity requirements. The Mission Owner may require the use of a stronger I&A technology. ▪ Privileged user’s access to administer Mission Owner systems/applications instantiated on IaaS/PaaS requires the use of DoD CAC/PKI or Alt Token/PKI. DoD ECA PKI certificates may be used by DoD contractor personnel if a physical token cannot be provided. 	<ul style="list-style-type: none"> ▪ Mission Owner’s privileged user’s 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. DoD ECA PKI certificates may be used by DoD contractor personnel if a physical token cannot be provided. ▪ Non-privileged user access to non-publicly released non-CUI information in the CSP’s SaaS offering minimally requires I&A through the use of a UID and password that meets DoD length and complexity requirements.
Level 4 and 5	<ul style="list-style-type: none"> ▪ Non-privileged user access to CUI and/or unclassified NSS (L5) requires the use of DoD CAC/PKI. DoD ECA PKI certificates may be used by DoD contractor personnel if a physical token cannot be provided. 	<ul style="list-style-type: none"> ▪ Mission Owner’s privileged user’s 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. DoD ECA PKI certificates may be used by

	<ul style="list-style-type: none"> ▪ Privileged user’s access to administer Mission Owner systems/applications instantiated on IaaS/PaaS requires the use of DoD CAC/ PKI or Alt Token/PKI. DoD ECA PKI certificates may be used by DoD contractor personnel if a physical token cannot be provided. 	<p>DoD contractor personnel if a physical token cannot be provided.</p> <ul style="list-style-type: none"> ▪ Non-privileged user access to CUI and/or unclassified NSS (L5) information in the CSP’s SaaS offering requires the use of DoD CAC/PKI. DoD ECA PKI certificates may be used by DoD contractor personnel if a physical token cannot be provided.
Level 6	<ul style="list-style-type: none"> ▪ Non-privileged user access to classified information requires the use of NSS SIPRNet Token/PKI ▪ Privileged user’s access to administer Mission Owner systems/applications instantiated on IaaS/PaaS requires the use of NSS SIPRNet Token/PKI. 	<ul style="list-style-type: none"> ▪ 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. ▪ Non-privileged user access to classified information in the CSP’s SaaS offering requires the use of NSS SIPRNet Token/PKI

NOTE: Mission Owners 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.

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 CSP customer's / Mission Owner’s systems.

- **Impact Level 2:** IAW 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
- **Impact Level 4 and 5:** IAW DoD policy the CSP must implement DOD ECA/PKI authentication for CSP privileged user access to administer and maintain dedicated CSP infrastructure supporting DoD contracted services.
- **Impact Level 6:** IAW 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 services.

5.4.2 Public Key (PK) Enabling

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

- Identifying themselves to other hosts.

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

The IASE web site page [Public Key Infrastructure \(PKI\) and Public Key Enabling \(PKE\)](#)¹⁰ provides all the information needed to PK enable Mission Owner's systems/applications instantiated on CSP's IaaS/PaaS offerings and CSP's PK enabling of SaaS offerings and service ordering/management portals/interfaces. This includes information regarding integration with the DoD PKI and the NSS PKI which is managed by DISA for the CNSS.

5.5 Policy, Guidance, Operational Constraints

DoD-specific policy, guidance and operational constraints must be followed as appropriate by CSPs. The Broker will evaluate equivalencies on a case by case basis.

5.5.1 SRG/STIG Compliance

CSPs are subject to the FedRAMP selected security control SP 800-53 CM-6. STIGs and/or SRGs may be used to fulfill this baseline configuration requirement. STIGs are applicable if the CSP utilizes the product the STIG addresses. SRGs are applicable in lieu of STIGs if the CSP utilizes the technology a SRG addresses and a product specific STIG is not available. However, the SP 800-53 control applies whether or not a STIG or SRG is available. The full list of STIGs and SRGs can be found on DISA's IASE web site.¹¹

CSPs must utilize all applicable DoD SRGs and STIGs to secure all DoD contracted cloud computing services provided on dedicated infrastructure. This applies at levels 4 and above for IaaS, PaaS, and SaaS offerings.

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

5.6 Physical and Personnel Requirements

Impact Level 5 and 6 CSPs are required to handle DoD classified information, either as part of DIB CS/IA membership, or in the case of Impact Level 6, in the form of DoD customer data. To be able to access classified data, CSPs must participate in the National Industrial Security Program. (NISP) The requirements for NISP are outlined in DoD 5220.22M – the National Industrial Security Program Operating Manual (NISPOM)¹².

DIB CS/IA membership and CSP facilities with classified information must acquire a Facility Security Clearance and ensure that all personnel handling classified information are cleared to the appropriate level.¹³

{Place holder for personnel requirements}

¹⁰ <http://iase.disa.mil/pki-pke/Pages/index.aspx>

¹¹ <http://iase.disa.mil/stigs/Pages/index.aspx>

¹² NISPOM: <http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>

¹³ DSS Facility Clearance Branch: http://www.dss.mil/isp/fac_clear/fac_clear.html

NOTE: 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 a CSP's employee can have on DoD mission or data.

From a DoD policy perspective, high risk positions include those in which an individual is responsible for the planning, direction, and implementation of a computer security program; 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. Such positions require the individual to undergo a Background Investigation in accordance with DoD personnel security policies.

As the DoD looks to leverage the benefits of the commercial cloud space, we must maintain an appropriate level of security; minimizing the risk of the insider threat while not imposing requirements that provide little to no benefit and increase costs. As a general rule, the risk will increase both as the Impact Level gets higher and the responsibilities of the CSP move further towards the data (e.g. IaaS → PaaS → SaaS).

During this comment period, DoD seeks information from the CSP community on the applicability of this requirement to their personnel across the various Impact Levels and types of service; along with possible compensating controls that are or could be in use today to minimize the risk of a rogue insider.

5.7 Data Spill

Per CNSSI 4009, IA Glossary, a data spill or “spillage” is an unauthorized transfer of classified data 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 an incident that requires an immediate response from both the mission owner and CSP in order to minimize the scope of the spill and the risk to DoD data. Cloud environments present a unique challenge for data spill response. Data spills are typically remediated or “cleaned” by sanitizing affected hardware to ensure that reconstruction of spilled data is impossible or impractical. This process, however, frequently requires that affected resources be 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 virtualization may make physical data locations difficult to ascertain, further complicating spill cleanup.

Variability in CSP infrastructures precludes the possibility of establishing a single cleanup process. Instead, CSPs will be responsible for providing methods and timelines for deleting specified units of data within their infrastructure in a way that provides high assurance that such data cannot be reconstructed. An example of such a process is:

- Volatile hardware with subject data will be powered down within 24 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.

- Unencrypted subject data locations on nonvolatile storage hardware will be overwritten or “cleared” as defined in NIST 800-88 within 24 hours, subject to exceptions based on potential side effects of cleanup actions. Encrypted subject data will be deleted cryptographically by destroying the appropriate decryption keys, then “cleared” and overwritten.
- Affected nonvolatile storage hardware will be tracked and destroyed at the end of its useful life.

These methods will be evaluated as part of the PA assessment, and then made available to all mission owners utilizing that CSP. The CSP will be responsible for executing any of those methods upon report of a data spill by a mission owner.

5.8 Data Removal/Recovery and Destruction

For the purpose of this section, Data Removal/Recovery refers to a Mission Owner requiring the removal of data stored in a CSP’s infrastructure for the purpose of transferring it to a different storage facility. Destruction of the data is required subsequent to successful transfer.

Upon request by a Mission Owner, the CSP will make all Mission Owner data stored in SaaS offerings available for electronic transfer out of the CSP environment, with subsequent destruction, within 60 days from the date of request. Each DoD cloud customer may also request different means of data transfer (for example, as called out in the SLA), at its discretion. The subsequent destruction of transferred data must include all CSO backups or mirrored storage maintained by the CSP. The CSP will provide assurance of data destruction.

DoD Mission Owners using IaaS/PaaS offerings, by the nature of the CSO are typically capable of removal/recovery of their data at any time with the exception of CSO backups or mirrored storage maintained by the CSP. Upon request by a DoD Mission Owner, the CSP will destroy all CSO backups or mirrored storage maintained by the CSP within 60 days from the date of request. The CSP will provide assurance of data destruction.

To support removal/recovery/destruction of any CSP customer data, the CSP should segregate the storage of customer data by customer. While this is typical for IaaS/PaaS, it may not be for SaaS where it is most important.

If an Impact Level 2-5 CSP plans to reuse storage hardware containing DoD data at a different sensitivity level, after requested data is successfully transferred from the CSP to DoD, CSP will “Purge” all instances of such data from its systems to include all backups, in accordance with NIST 800-88 and the FedRAMP selected security control MP-6. Alternatively, the CSP may provide some equivalent assurance of data destruction, for which approval will be at the discretion of the Mission Owner/Data Owner.

Impact Level 6 CSPs may not reuse storage hardware at a different sensitivity level. This processing and storage hardware will be sanitized in accordance with NSA/CSS Storage Device Declassification Manual 9-12¹⁴.

¹⁴ http://www.nsa.gov/ia/ files/Government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf

5.9 Disposal of Storage Hardware

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

Impact Level 2-5 CSP will ensure this by, at minimum, “Purge” all data on devices prior to disposal, reuse, or transfer, in accordance with NIST 800-88. Devices that are unable to be cleared or purged must be physically destroyed, as defined in NIST 800-88. When there is any doubt to the success of the cleared or purged process, the storage device must be destroyed in accordance with NIST 800-88.

Impact Level 6 CSP will ensure classified data is irretrievable by sanitizing devices in accordance with NSA/CSS Storage Device Declassification Manual 9-12¹⁴.

5.10 Architecture

This section of the Cloud Computing SRG provides guidance on the various architectural considerations related to DoD’s use of commercial cloud services in the following areas:

- The connection between the CSP’s infrastructure and the DoD Information Network (DoDIN)
- CSP service protections and integration into required DoDIN CND and access control services
- CSP’s customer’s system/application protections and integration into required DoDIN CND and access control services

5.10.1 Cloud Access Point

The DoD Cloud Access Point (CAP) is system of network boundary protection and monitoring devices, otherwise known as an IA stack, through which all CSP infrastructure connects to a DoD Information Network (DoDIN) service, the Non-secure Internet Protocol Router Network (NIPRNet), or Secret Internet Protocol Router Network (SIPRNet). The CAP will change character depending upon where the cloud infrastructure is on or off premises. There are internal CAPs (ICAPs) and DoDIN/NIPRNet/SIPRNet Boundary CAPs (BCAPs).

CSP Infrastructure (dedicated to DoD) located inside the B/C/P/S “fence-line” (i.e., on-premises) connects via an ICAP. The architecture of ICAPs may vary and may leverage existing capabilities such as the IA Stack protecting a DoD Data center today or may be a Joint Regional Security Stack (JRSS). On the other hand, an ICAP may have special capabilities to support specific missions or CSP types or services.

CSP Infrastructure (shared w/ non-DoD or dedicated to DoD) located outside the B/C/P/S fence-line which connects to the DoDIN/NIPRNet does so via one or more BCAPs. The BCAP terminates dedicated circuits and VPN connections originating within the CSP’s network infrastructure and/or Mission Owner’s virtual networks. All connections between CSP’s network infrastructure or Mission Owner’s virtual networks that is accessed via or from the NIPRNet/SIPRNet must connect to the DoDIN via a BCAP.

- **Level 2:** All traffic to and from CSP infrastructure serving Level 2 missions and the mission virtual networks will connect via the Internet. The BCAP is not used. See section 5.10.3.2, “Management Plane Connectivity” for additional details.

- **Level 4 and 5:** All traffic to and from CSP infrastructure serving Level 4 and level 5 missions and the mission virtual networks must connect via one or more BCAPs. This includes the production plane for non-privileged user access and the management plane for privileged user access and IA/CND tool reach-back. See sections 5.10.3.1, “User/Data Plane Connectivity” and 5.10.3.2 Management Plane Connectivity for additional details. High availability Mission Owner systems and their supporting CSP network infrastructure must connect to two or more BCAPs. The BCAP will support Internet facing Mission Owner systems IAW the DMZ STIG.
- **Level 6:** All traffic to and from CSP infrastructure serving Level 6 missions and the mission virtual networks must connect via one or more BCAPs to the SIPRNet instead of the NIPRNet. This includes the production plane for non-privileged user access and the management plane for privileged user access and IA/CND tool reach-back. See section 5.10.3.1, “User/Data Plane Connectivity” and 5.10.3.2, “Management Plane Connectivity” for additional details. High availability Mission Owner systems and their supporting CSP network infrastructure must connect to two or more BCAPs.

[Placeholder for one or more drawings]

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.

5.10.3 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 router. The network plane in general is subject to the network related DoD SRGs and STIGs. This Cloud Computing SRG does not contain additional requirements related to network plane connections to the cloud computing infrastructure.

5.10.3.1 User/Data Plane Connectivity

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

Table 5 - User/Data Plane Connectivity

Impact Level	Off-Premises	On-Premises
	Non-DoD CSP Service Offering Infrastructure	DoD and Non-DoD CSP Service Offering Infrastructure
Level 2	<ul style="list-style-type: none"> ▪ User connectivity will leverage commercial infrastructure (i.e., Internet). ▪ Users connecting from the Internet will connect directly while users 	<ul style="list-style-type: none"> ▪ User connectivity will use existing infrastructure (Government owned) for its user/data plane when the user is within the B/P/C/S fence-line (on-premises) and directly connected to the

	<p>connecting from the DoDIN (i.e., NIPRNet) will connect to the Internet via the DoDIN Internet Access Points (IAPs).</p> <ul style="list-style-type: none"> ▪ CSO connections will be assessed and authorized using the same external connection requirements as any other Internet-facing connection. 	<p>local Base Area Network (BAN) and NIPRNet.</p> <ul style="list-style-type: none"> ▪ 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 DoDIN Internet Access Points (IAPs) then an ICAP.
<p>Level 4 And 5</p>	<ul style="list-style-type: none"> ▪ User connectivity will leverage a DoDIN 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 DoDIN 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 DoDIN extension will traverse a BCAP. ▪ Users connecting from the DoDIN (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 the same as any other internal connection using the same requirements as any other Internet-facing connection (i.e., IAW the DMZ STIG). 	<ul style="list-style-type: none"> ▪ CSO connections will be assessed and authorized the same as any other internal connection.
<p>Level 6</p>	<ul style="list-style-type: none"> ▪ User connectivity will leverage a DoDIN extension to the commercial facility using government SECRET network infrastructure within government boundaries (i.e. SIPRNet) and commercial infrastructure beyond government boundaries (i.e. commercial carrier infrastructure / connectivity service offerings). ▪ The DoDIN extension to a commercial 	<ul style="list-style-type: none"> ▪ 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 will use Type 1 encryption or commercial equivalent (CSfC Suite B) and must enter/leave the SIPRNet via the

	<p>facility can be accomplished with a Multiprotocol Label Switching (MPLS) router and optical switch (referred to as a Service Delivery Node). The DoDIN extension will traverse a BCAP and will use Type 1 encryption or commercial equivalent (CSfC Suite B).</p> <ul style="list-style-type: none"> User traffic to/from the Internet will use Type 1 encryption or commercial equivalent (CSfC Suite B) and must enter/leave the SIPRNet via the SIPRNet to Internet gateways then a BCAP. 	<p>SIPRNet to Internet gateways then an ICAP.</p> <ul style="list-style-type: none"> CSO connections will be assessed and authorized the same as any other internal connection using the same requirements as any other Internet-facing connection (i.e., IAW the DMZ STIG).
--	--	---

5.10.3.2 Management Plane Connectivity

The management plane carries network/server/system privileged user (administrator) traffic along with maintenance and monitoring traffic. . Table 6 details the management plane connectivity by impact level for Mission Owner’s systems/applications and CSP’s CSOs.

Table 6 - Management Plane Connectivity

Impact Level	Mission Owner Management Plane	CSP Service Offering Management Plane
Level 2	<ul style="list-style-type: none"> Management connectivity from inside the NIPRNet 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 be natively encrypted or must traverse a VPN connection. All traffic must enter/leave the NIPRNet via the DoDIN Internet Access Points (IAPs) Management connectivity by DoD personnel or DoD contractors from outside the NIPRNet requires an encrypted, tunneled connection directly via the Internet to the mission system/application and virtual network. Management traffic to CSP service 	<ul style="list-style-type: none"> DoD CSP on-premises service offering infrastructure and management: CSP management connectivity will utilize existing infrastructure such as the Enterprise Services Directorate (ESD) Out of Band (OOB) management network. No service provider security stack is required. 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 and will be used to access remote service

	<p>ordering / service management portals must be encrypted if not in an encrypted VPN. Monitoring traffic must be natively encrypted or must traverse a VPN connection. All traffic entering/leaving the NIPRNet must be via the DoDIN Internet Access Points (IAPs)</p>	<p>offering infrastructure.</p> <ul style="list-style-type: none"> ▪ Non-DoD CSP on-premises service offering infrastructure and off-premises management: CSP management connectivity can leverage an encrypted, tunneled connection from the CSP's off-premises management infrastructure to the service provider's on-premises service offering infrastructure
<p>Level 4 And 5</p>	<ul style="list-style-type: none"> ▪ Management connectivity from inside the NIPRNet requires an encrypted, tunneled connection through the NIPRNet and an ICAP or BCAP to manage the mission system/application and virtual network. Management traffic to CSP service ordering / service management portals must be encrypted if not in an encrypted VPN. Monitoring traffic must be natively encrypted or 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 requires an encrypted, tunneled connection from the Internet via an IAP and an ICAP or BCAP to 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 be natively encrypted or must traverse a VPN connection via a BCAP and NIPRNet. 	<ul style="list-style-type: none"> ▪ 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 separate.
<p>Level 6</p>	<ul style="list-style-type: none"> ▪ All management and monitoring connectivity is via the SIPRNet. Management and monitoring traffic should be encrypted using FIPS validated cryptography to accommodate separation for Need-to know reasons. 	<ul style="list-style-type: none"> ▪ DoD CSP on-premises service offering infrastructure and management: CSP management connectivity will utilize existing SECRET network infrastructure such as the SECRET Out of Band (OOB) management network. No service provider security stack is required. ▪ Non-DoD CSP on-premises service

		<p>offering infrastructure and management: The CSP may directly connect their management infrastructure to their service offering infrastructure if personnel are collocated using their SECRET LAN. An encrypted, tunneled connection using FIPS 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.</p> <ul style="list-style-type: none">▪ Non-DoD CSP on-premises service offering infrastructure and off-premises management: CSP management connectivity can 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 should be separate.
--	--	---

5.10.4 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 hosts 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 (IDPS), and a De-Militarized Zone (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.

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. Equivalent alternative measures will be assessed on a case by case basis.

5.10.4.1 SaaS

Mission Owner users 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 that users place / process in the service and its 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 assessment for provisional authorizations for SaaS offerings and/or DoD component ATOs, defense-in-depth security / protective measures must be assessed for adequacy and potential risk acceptance by DoD. This may be in addition to assessing IA controls. Much of following guidance is reflected in the DoD DMZ STIG and Application Security and Development STIG along with other operating system (OS) and application specific STIGs.

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

- Application Layer Firewall (properly configured) and IDPS protection of the CSP's infrastructure supporting the SaaS application offering as well as segmentation from the CSP's other offerings and corporate networks.
- Application / network architecture which provides 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.
- Customer data-at-rest encryption protections using FIPS 140-2 validated crypto modules operated in FIPS mode.
- Customer data-in transit encryption protections using FIPS 140-2 validated crypto modules operated in FIPS mode.
- Hardening / patching / maintenance of OSs and applications. DoD SRGs and STIGS may be used, and must be used if the service is private DoD or a Federal Government Community used by DoD.
- 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.

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

[Place holder for a drawing]

5.10.4.2 IaaS/PaaS

Mission Owners build systems and applications on virtual infrastructure provided by the CSP service offering under IaaS/PaaS and are responsible for their security. Under PaaS, there may be a delineation of responsibility for security between the CSP and the CSP's customer depending

upon how the CSP presents its PaaS offering (e.g., the security features it includes). Under IaaS the Mission Owner is fully responsible for securing the operating systems and applications that they build on the service offering. For the purpose of this section of the CSM, IaaS and PaaS offerings are treated the same. The Mission Owner might inherit mitigations that the CSP provides toward meeting their defense-in-depth security / protective requirements.

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 5.10.7, “Mission Owner System/Application Architecture using IaaS/PaaS.”

NOTE: equivalencies to the vulnerability mitigations provided in DoD SRGs and STIGS that are incumbent upon the CSP’s DoD customer may be viable and acceptable but must be approved by the DISA AO.

5.10.5 IP Addressing and DNS

DoD policy and the DNS STIG require all DoD ISs to use the DoD authoritative DNS servers, not public or commercial DNS servers. Additionally it requires all DoD IS to be addressed in the .mil domain. Mission Owners are not authorized to utilize DNS services offered by the CSP or any other non-DoD DNS provider.

This affects DoD IS instantiated on commercial cloud infrastructure as follows:

- **Impact Level 2:** DoD IS implemented at level 2 will be instantiated in commercial CSP facilities with direct access from the Internet. As such they will be addressed using public IP addresses assigned and managed by the CSP. In order for these systems to comply with DoD DNS policy, they must use a C-Name in the system’s authoritative DNS record in the DoD authoritative servers that points to the CSP assigned public IP address.
- **Impact Levels 4 and 5:** DoD IS implemented at levels 4 and 5 instantiated in commercial CSP facilities will be treated and designed as an extension of the NIPRNet and will be addressed using DoD assigned and managed IP addresses. These systems will use the DoD authoritative DNS servers on the NIPRNet IAW policy as would any other DoD IS. NIPRNet addresses are assigned by the DoD NIC.
- **Impact Level 6:** DoD IS implemented at level 6 instantiated in commercial CSP facilities will be treated and designed as an extension of the SIPRNet and will be addressed using SIPRNet IP addresses. These systems will use the DoD authoritative DNS servers on the SIPRNet IAW policy as would any other SIPRNet connected IS. SIPRNet addresses are assigned by the DoD NIC.

5.10.6 Mission Owner Architecture using SaaS

While Defining the SaaS architecture is the responsibility of the CSP, Mission Owners contracting for and using CSP’s SaaS offerings must minimally address the following to meet DoD policy:

- Register the Protocols and Services along with their related IP Ports used by the SaaS service that will traverse the DoDIN. This includes all traffic for Levels 4, 5, and 6 as well as management plane traffic for Level 2.
- Register the service/application with the DoD whitelist for both inbound and outbound traffic.

As discussed in section 5.10.4, “CSP Service Architecture”, the Mission Owner is reliant on the security posture of the CSP and their SaaS offering for the protection of DoD data/information.

5.10.7 Mission Owner System/Application Architecture using IaaS/PaaS

Most of the areas of concern for implementing defense-in-depth security / protective measures that a Mission Owner must address when implementing systems/applications on IaaS / PaaS include, but are not limited to, the following; which generally applies to all information impact levels unless specifically stated otherwise:

- 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 normally approved architecture for the type of application as defined in the DoD DMZ STIG and Application Security and Development STIG along with other operating system and application specific STIGs. For example, a web service or application is typically required to have unrestricted/restricted DMZ zones with appropriate protections for internet/externally facing servers and private / “back end” zones with appropriate protections for application/database servers and other supporting systems/servers.
- For shared infrastructure with direct Internet access (Level 2): Implement virtual application level firewall and virtual IDPS capabilities IAW the applicable DoD SRGs and STIGs to protect the virtual network(s) and interconnected VMs. This is possible because just about every firewall/IDS vendor has virtual versions of their IA appliances. This might be accomplished in its own virtual network with other virtual networks “connected” behind it. Proxy VMs if applicable might be implemented in this virtual network.
NOTE: It must be assumed that the CSP does not provide significant firewall capabilities between the Internet and their IaaS/PaaS offerings so that they may support the needs of many more customers. Even if they do, the CSP may not be responsive about changing firewall rules when requested by one customer if others use the same gateway. The Mission Owner and/or their CNDSP must be able to control firewall rules and monitor the virtual network boundary.
- For shared or dedicated infrastructure with a DoDIN connection (Levels 4-6): implement firewall and/or routing methods that restrict traffic flow inbound and outbound to/from the virtual network to the DoDIN connection. 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 between the virtual firewall, the virtual IDS capabilities and the CNDSP responsible for the mission system/application. See section 6, “COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE” for more specific information.
- Harden (STIG) / patch / maintain each VM’s OS under IaaS and PaaS IAW DoD policy and CYBERCOM direction. The use of DoD STIGs and SRGs is required for hardening.
- Harden (STIG) / patch / maintain each application provided by the CSP under PaaS IAW DoD policy and USCYBERCOM direction. The use of DoD STIGs and SRGs is required for hardening.

- 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 hardening as is compliance with IAVMs.
- Implement data-at-rest encryption on all DoD files housed in CSP IaaS storage service offerings. A CSP may offer one or more services or methods to accomplish this. Data-at-rest encryption may help mitigate issues with data/information spillage.
IF the DoD information is sensitive (e.g., FOUO or CUI) this encryption must use FIPS 140-2 validated software crypto modules operated in FIPS mode. While this is required for “sensitive government information”, it is best to also encrypt public information at rest in CSP IaaS storage service offerings to protect its integrity.
- Implement HBSS IAW DoD policy.
 - Implement HBSS McAfee agents on all VMs with a general purpose OS.
 - Utilize an EPO server within NIPRNet.
 - Implement a secure (encrypted) connection or path between the HBSS McAfee agents and their EPO server.
 - Provide visibility by the Mission Owner’s CNDSP entities as defined in section 6, “COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE.”
- Implement an ACAS server IAW USCYBERCOM TASKORD 13-670.
 - Implement a secure (encrypted) connection or path between the ACAS server and its assigned ACAS Security Center.
 - Provide visibility by the Mission Owner’s CNDSP entities as defined in section 6.
- Implement DoD PKI server certificates for establishing secure connections.
- Implement all required data-in-transit encryption protections using FIPS 140-2 validated crypto 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 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 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.
- Register the Protocols and Services along with their related IP Ports used by the Mission Owner’s system/service/application that will traverse the DoDIN. This includes all traffic for Levels 4, 5, and 6 as well as management plane traffic for Level 2.
- Register the Mission Owner’s system/service/application with the DoD whitelist.

NOTE: A Mission Owner may contract the CSP to harden (STIG) / patch / maintain VMs, OSs, or applications, or maintain STIGed and patched VM images for use if the CSP provides such a service. Such services must be validated as equivalent to DoD standards IAW all applicable policies.

[Placeholder for a drawing]

DRAFT

6 COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE

Maintaining a strong defensive capability with effective command and control structures, along with ensuring visibility of cyber related information, are key challenges in DoD's adoption of cloud services. Computer Network Defense (CND) addresses the defense and protection of networks and Information Systems (ISs), detection of threats, and response to incidents. Cyber Situational Awareness (CSA) improves the quality and timeliness of collaborative decision-making regarding the employment, protection, and defense of DoD systems and data. The CND Command and Control (C2) structure provides the means to react to threats and incidents to defend the DoD Information Networks (DoDIN).

6.1 Overview of CND Tiers

DoD operates a tiered CND Command and Control (C2) structure. The structure consists of USCYBERCOM at the top tier (Tier 1) and a network of CND Service Providers (CNDSPs) (Tier 2) that have been accredited by USCYBERCOM IAW DoD policy. Each DoD information system is operated/managed by a Mission Owner (Tier 3) which must be aligned with an accredited CNDSP which monitors and protects the information systems and associated assets. CNDSPs report information to USCYBERCOM which maintains Cyber Situational Awareness over all DoD networks and ISs. USCYBERCOM also provides threat information collected from various sources and threat mitigation orders to the CNDSPs and mission owners.

DoD is adjusting its CND C2 structure to include Joint Force Head Quarters (JFHQ) – DoD Information Network (DoDIN) in conjunction with the migration to the Joint Information Environment (JIE). As the JFHQ moves into operation, certain responsibilities may shift from USCYBERCOM at Tier 1.

6.2 Concept Changes for Tiers for Cloud Computing

Defending the DoDIN while integrating cloud computing requires new constructs within the CND C2 structure, including the identification of entities with new Tier 2 CND Command and Control (C2) and Operations (Ops) responsibilities. The use of a Cloud Access Point (CAP) drives the requirement for two distinct functions/roles: Boundary CND and Mission CND.

6.2.1 Boundary CND

Boundary CND (BCND) monitors and defends the connections to/from off-premises CSPs at the BCAP(s) for dedicated circuits or a VPN connections. This effort is primarily focused on managing the overall risk that the CSP connection poses to the DoDIN but also provides benefits to the Mission Owners. CND Command and Control (C2) and Operations (Ops) responsibility for protecting the DoDIN is -that of the DISA Command Center (DCC) and DISA NetOps Center (DNC) Continental US (CONUS). An additional function of BCND includes cross-CSP analysis activities. Given that a single CSP may support multiple mission systems for different DoD Mission Owners, DOD must address potential impacts across the multiple missions supported by that CSP; ensuring that Mission Owners and supporting Mission CND have situational awareness for more global risks.

Boundary CND (BCND) also monitors and defends the connections to/from on-premises CSPs at the ICAPs. This may be performed by or in conjunction with the Mission CNDs.

6.2.2 Mission CND

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

6.3 CND Roles and Responsibilities

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

- **Boundary CND (BCND):** A Tier 1 and Tier 2 function of DNC CONUS and the DISA Command Center (DCC) focused on DoD's use of cloud computing and commercial CSPs.
 - Responsible for protecting the DoDIN and DoD mission systems in commercial cloud infrastructure via the Cloud Access Point (CAP)
 - Coordinates communications between USCYBERCOM and MCNDs
 - Responsible for monitoring CSP adherence to incident response processes and advising the CSPs on protecting their infrastructure and the DoD mission systems that they host.
 - Serves as the CSP's single DoD point of contact (POC) and directs C2 actions regarding DoDIN-wide incident and system health reporting involving a CSP.
 - Establishing and maintaining external communications with the CSP and ensuring the internal DoD communications are established between all entities which include the MCND and BCND
- **Mission CND (MCND):** Tier 2 responsibilities integrated in the existing DoD CNDSPs focused on cloud computing. MCND is minimally responsible for:
 - Monitoring, protecting, and defending the Mission Owner's cloud-based systems, applications, and virtual networks in the CSP's IaaS/PaaS infrastructure.
 - Ensuring internal DoD communications are established between all entities which include the Mission Owner, MCND, and BCND.
- **Mission Administrators:** Administrators of Mission Owner's cloud-based systems, applications, and virtual networks; a Tier 3 entity consuming CNDSP services; minimally responsible for:
 - Following Tier 1 and Tier 2 direction (C2)
 - 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
- **The CSP:** While CSPs provide for their own CND services, CSPs will effectively function as a Tier 3 entity within the DoD CND architecture to provide for a secure environment for Mission Owner's systems, applications, and virtual networks. CSPs are minimally responsible for:

- Providing local operational direction and support for CND within their infrastructure and service offerings
- Fully maintaining, patching, monitoring, and protecting the infrastructure supporting all service offerings.
- Fully maintaining, patching, monitoring, and protecting SaaS service offerings's OSs and applications including DoD data/information in them.
- And as contracted:
 - Coordinate with the BCND regarding incident response and the mitigation of threats to DoD clouf based mission systems/applications and data.
 - Providing timely incident and system health reports
 - Maintaining bidirectional Cyber Situational Awareness
- **Mission Owners:** Individuals/organizations responsible for the overall mission environment; ensuring that the functional requirements of the system are being met; Are minimally responsible for:
 - Engaging and funding the services of a MCND to provide for the defense of the Mission Owner's systems, applications, and virtual networks in any CSP's IaaS/PaaS infrastructure (whether DoD operated or operated by a commercial/non-DoD entity).
 - Negotiating the terms and requirements with the CSP for incident reporting and incident response, in coordination with the BCND and their MCND provider.

Figure 8 provides a graphic representation of these entities and the flow of communications between them.

DRAFT

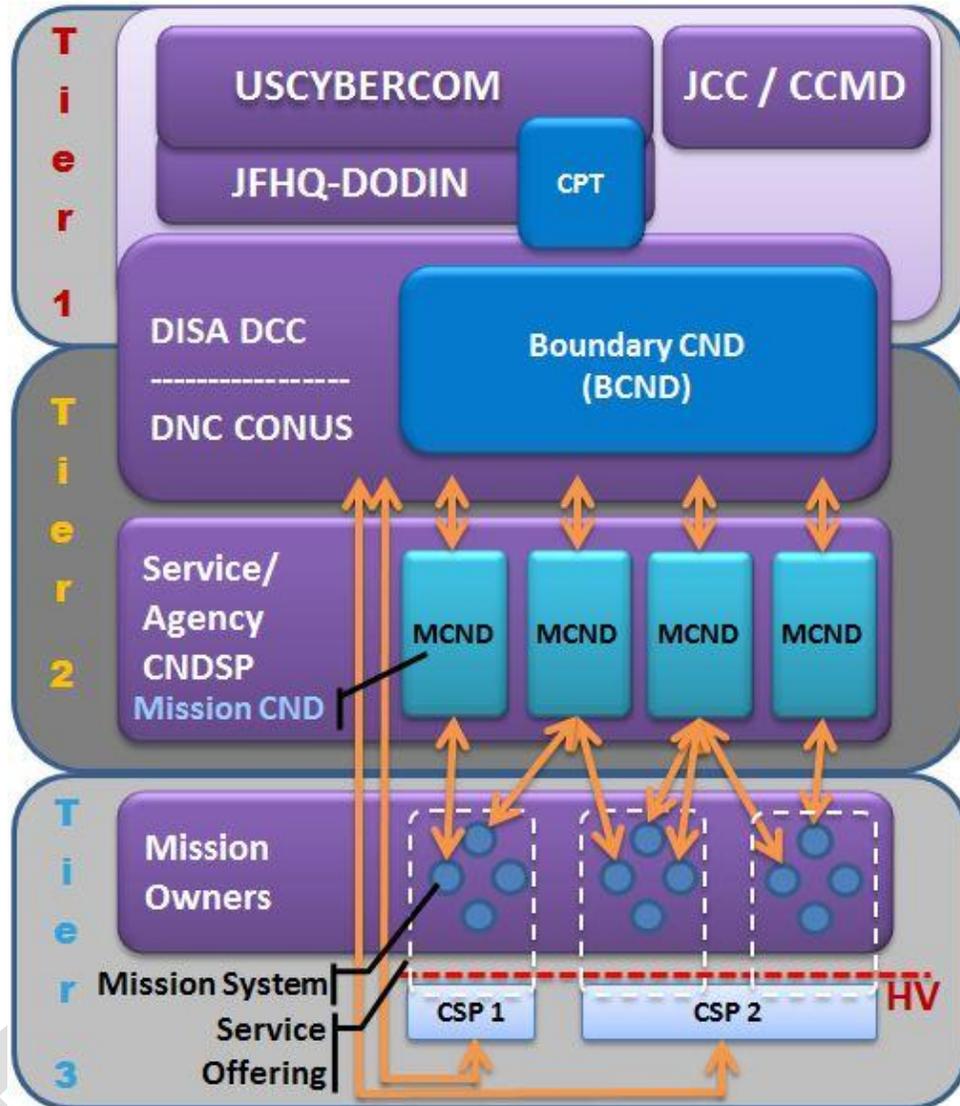


Figure 8 – DoD Cloud Incident Response and CND C2 Structure

6.4 Incident Reporting and Response

FedRAMP, through the selection and implementation of IR-6, requires CSPs to report incidents to the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team¹⁵ (US-CERT) and the consuming Federal Agencies. For Cloud Service Offerings (CSOs) that are multi-tenant or otherwise shared across Federal Agencies outside of the DoD (Impact Level 2), incidents will be reported to US-CERT in compliance with FedRAMP requirements in parallel with the DoD reporting requirements. For CSOs that providing dedicated infrastructure to the DoD (Impact Levels 4,5,6), incidents regarding that infrastructure and CSO will not be reported to US-CERT, but directly to the DoD unless the infrastructure is shared with other

¹⁵ <https://www.us-cert.gov/>

Federal Government tenants. The DoD Tier 1 (USCYBERCOM) will handle coordination with US-CERT and other entities as appropriate.

All CSOs actively supporting DoD missions will be supported by the BCND. The BCND will be the DoD point of contact to whom the CSP's Operational entity will report incidents affecting the security posture of the CSP and the CSP's cloud service offerings. The CSP will coordinate its response to such incidents with BCND. The BCND will coordinate with all related MCNDs that are servicing mission systems operating under the CSP.

6.4.1 DoD Command and Control and Network Operations Integration

CSPs will be integrated within the overall DoD Command and Control (C2) and Network Operations (NetOps) structure, to include integration with USCYBERCOM defense operations via BCND services. In general, the degree of integration required between a CSP and DoD C2 and NetOps increases with higher impact levels.

CSPs will provide an *Incident Response Plan Addendum* to document their approach in fulfilling these integration requirements. CSPs will make their plan addendum available to the Broker 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* in conjunction with updates and deliveries of their *Incident Response Plan*, as required by the FedRAMP selected security control IR-1. A CSP's plan addendum must specifically address data breaches, where a "breach" 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 addendum addresses all breaches regardless of the time, day, or location of the breach, and must provide for notice to the Government of any breach of its data. The plan addendum must incorporate any other policies or procedures that the Government may require to be followed in the event of a breach, including, but not limited to:

- How and to whom within the Government, the breach will be reported;
- Specific steps to be taken in order to mitigate or remedy the breach, including time periods for taking such steps (e.g., reporting of Personally Identifiable Information (PII) data breaches within one hour);
- How and under what circumstances any affected individuals or entities by a breach will be notified, and by whom; and
- Any other special instructions for handling computer security incidents affecting, or potentially affecting, U.S. Government data, consistent with guidance and policy directives issued by DoD, NIST, and US-CERT for incident management, classification, and remediation, National Instruction on Classified Information Spillage issued by the CNSS, or other applicable law, regulation, order or policy.

6.4.2 Information Requirements, Categories and Timelines

CND Tier 1, the BCND and MCNDs develop Information Requirements that identify the information necessary to accomplish their mission. CSPs are responsible for providing information to the BCND that fulfills those information requirements. In the course of a CSP performing CND for its environments, CSPs will monitor their information systems, and report relevant information to the BCND. The following are groups of information requirements relevant to CSP operations.

Threat Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The threat vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive.
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack does not fit into any other vector	

Service outage with mission impact (e.g., scheduled maintenance, natural disasters), Incident categories and required reporting timelines from the CSP to the BCND are defined in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B¹⁶, Appendix A to Enclosure C – Reporting Timelines. These categories are part of the implementation required by the FedRAMP selected security control IR-4 and the Broker selected security control enhancement IR-4(3). The categories of reports that are required from a CSP will vary by impact level and are documented, along with required notification times in Table 7.

¹⁶ CJCSM 6510.01B: http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

Table 7 – Incident Categories per Impact Level

Incident Category	Description	Notification Time Requirement Impact Level 2	Notification Time Requirement Impact Level 4	Notification Time Requirement Impact Levels 5-6
1	Root Level Intrusion	2 Hours	2 Hours	2 Hours
2	User Level Intrusion	2 Hours	2 Hours	2 Hours
3	Unsuccessful Activity Attempt	-	4 Hours	4 Hours
4	Denial of Service	Low: As directed by DoD Sponsor Mod/High: 15 Minutes	15 Minutes	15 Minutes
5	Non-Compliance Activity	-	4 Hours	4 Hours
6	Reconnaissance	-	-	4 Hours
7	Malicious Logic	2 Hours	2 Hours	2 Hours
8	Investigating	-	-	-
9	Explained Anomaly	-	-	-

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

6.4.3 Incident Reporting Mechanism

CSPs will submit reports using the most protected and secure means available for the affected information system. CSPs will use unclassified reporting mechanisms, such as the DoDIN encrypted email, non-secure phone/fax only for incidents on unclassified information systems in accordance with CJCSM 6510.01B, Enclosure C, Section 4 and Table C-1¹².

When classified incident reporting is appropriate and directed, CSPs will use SIPRNet email, or secure phone/fax to report and coordinate incidents as specified. This will always be the case for Level 6 reporting.

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 CND information may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

6.4.4 Incident Reporting Format

CSPs will apply the template format specified in CJCSM 6510.01B, Appendix B to Enclosure C, Section 1 – General Cyber Incident Report Format¹⁷ when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. 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.

¹⁷ CJCSM 6510.01B: http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

6.5 Warning, Tactical Directives, and Orders

The DoD operates a tiered CND C2 structure in order to effectively defend DoD information systems that are networked globally across a diverse set of environments. Each of these environments must defend the network and ensure the security of computing and communication systems. It is critical that certain information be disseminated; and that actions can be directed from higher levels of command to network defenders (which include CSPs providing services to the DoD).

CSPs must be able to receive, act upon, and report compliance with directives and notifications sent by CND Tier 2, as required by FedRAMP selected security control SI-5. These notifications may be generated by the Tier 1 or Tier 2 CND and may include guidance for or countermeasures to be taken by CSPs.

The DoD cyber chain of command for CSPs is represented in Figure 8. USCYBERCOM, at Tier 1, disseminates Warnings, Tactical Directives, and Orders to both the BCND and MCNDs (all Tier 2). The BCND entity for CSPs will receive those items and analyze them for their applicability to individual CSPs, as well as their need-to-know, then communicate with the CSPs involved. CSPs (effectively acting as Tier 3) will act to coordinate with the BCND, MCND and mission owners as contracted to implement the provided guidance and countermeasures.

6.6 Vulnerability Reporting / Plans of Action and Milestones (POA&Ms)

Understanding existing vulnerabilities/risks within the enterprise is a key component in performing effective CND analysis. The vulnerability reports and POA&Ms developed by the CSPs as part of both the FedRAMP and DOD requirements will be shared with BCND which will share with MCND providers for their collective use in providing CND.

6.7 Notice of Scheduled Outages

All CSPs must notify the affected MCND providers of planned system outages in advance and provide details on planned activities during the outage. Outages or changes that affect more than one instance of an offering must be reported to the BCND to enable broader situational awareness across all MCND providers.

6.8 PKI for CND Purposes

Impact Level 2 through 5: CSPs must have either a DoD PKI certificate or a DoD-approved ECA medium-assurance PKI Certificate¹⁸ for each person that needs to communicate with DoD via encrypted email.

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 CND personnel will use SIPRNet tokens/certificates to communicate with DoD via encrypted email.

¹⁸ DoD ECA PKI certificate: <http://iase.disa.mil/pki/eca/Pages/index.aspx>

6.9 CND Operations

DOD is developing event scenarios that outline where CND operational processes, procedures, and workflows will be documented to ensure standardization across CSP and DOD organizations. These will be defined in future updates to this document or in a companion document.

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. However, much of this information is classified.

6.10.1 Defense Industrial Base Cyber Security / Information Assurance Program

The Defense Industrial Base Cyber Security / Information Assurance Program¹⁹ (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. 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. Even though membership is voluntary under the DFAR, membership can be required in a contract. CSP participation in the DIB CS/IA program is mandatory for CSPs serving Impact Level 5 and 6 systems and applications. The purpose of mandating DIB CS/IA membership is to ensure that CSPs can receive and leverage cyber security threat information to protect infrastructure that hosts higher-value DoD data and systems. Access to classified information requires that Impact Level 5 and 6 CSPs implement the requirements contained in DoD 5220.22M – National Industrial Security Program Operations Manual (NISPOM).

NOTE: DoD CSPs are already integrated into the CND communications architecture and receive unclassified CYBERCOM notifications via those channels.

¹⁹ DIBNet CS/IA Portal: <http://dibnet.dod.mil/staticweb/index.html>

Appendix A References

1. CJCSM 6510.01B: Chairman of the Joint Chiefs of Staff Manual: Cyber Incident Handling Program, dated 10 July 2012.
http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf
 2. CNSSI 1253: Security Categorization and Control Selection for National Security Systems, dated 27 March 2014.
<https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
 3. CNSSI No.1253F, Attachment 5: Classified Information Overlay dated 09 May 2014.
<https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
 4. CNSSI No.1253F, Attachment x: Privacy Overlay dated TBD.
<https://www.cnss.gov/CNSS/issuances/Instructions.cfm> (when available)
 5. CNSSI 4009: National Information Assurance (IA) Glossary, dated 30 April 2010.
http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
 6. Executive Order 13526: Classified National Security Information, dated 29 December 2009.
<http://www.archives.gov/isoo/policy-documents/cnsi-eo.html>
 7. DRAFT: DoD Chief Information Officer, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, dated TBD
 8. DoDI 8500.01: Cybersecurity, dated 14 March 2014.
http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
 9. DoDI 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
 10. DoDI 8520.03: Identity Authentication for Information Systems, dated 13 May, 2011.
<http://dtic.mil/whs/directives/corres/pdf/852003p.pdf>
 11. Defense Information Systems Agency, DoD Enterprise Cloud Service Broker website.
<http://disa.mil/Services/DoD-Cloud-Broker>
 12. Federal Risk and Authorization Management Program (FedRAMP) Home Page
<http://cloud.cio.gov/fedramp>
 13. NIST SP 500-292: NIST Cloud Computing Reference Architecture, dated September 2011.
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
 14. NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, Revision 4, dated April 2013.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- Note: <http://csrc.nist.gov/publications/PubsSPs.html> contains additional documents relating to SP 800-53.

15. NIST SP 800-59: Guideline for Identifying an Information System as a National Security System, dated August 2003.
<http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf>
16. NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, dated October 2008.
<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>
17. NIST SP 800-88, Revision 1: Draft: Guidelines for Media Sanitization, dated September 2012.
http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
18. NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), dated April 2010.
<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
19. NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, dated December 2011.
<http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>
20. NIST SP 800-145: The NIST Definition of Cloud Computing, dated September 2011.
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
21. NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems, dated February 2010.
<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
22. Defense Information Systems Agency, the Security Technical Implementation Guide (STIG) Home Page
<http://iase.disa.mil/stigs/index.html>
23. Executive Order 12829 – National Industrial Security Program, dated January 1993.
<http://www.archives.gov/isoo/policy-documents/eo-12829.html>
24. DoD Instruction 5220.22: National Industrial Security Program, dated March 2011.
<http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf>
25. 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>
26. 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>
27. 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
28. 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

29. 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
30. DoD Manual 5200.2-R: Personnel Security Program, dated February 1996.
<http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf>
31. DSS Facility Clearance Branch
http://www.dss.mil/isp/fac_clear/fac_clear.html
32. DoD ECA PKI Certificate:
<http://iase.disa.mil/pki/eca/Pages/index.aspx>

DRAFT

Appendix B Definitions

Authenticity: 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: The property of being accessible and useable upon demand by an authorized entity.

Classified Data: Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD).

Cloud Broker: An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

CNDSP: Computer Network Defense Service Provider

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

Confidentiality: The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

Infrastructure as a Service (IaaS): A cloud service model focused on providing infrastructure required to host a workload; includes virtual machines, servers, storage, load, balancers, network, etc.

Integrity: 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.

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither may later deny having processed the data.

Platform as a Service (PaaS): A cloud service model focused on providing a suite of environment capabilities that enables the execution or development of applications; includes operating system, execution runtime, database, web server, development tools, etc.

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

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

Software as a Service (SaaS): A cloud service model focused on providing the full suite of products and applications to provide a service; includes email, virtual desktop, communication, applications, etc.

DRAFT

Appendix C Roles and Responsibilities

Table 8 provides a summary of the major roles and responsibilities in implementation of the Cloud Computing SRG.

Table 8 - Roles and Responsibilities

Role	Responsibility
Cloud Service Provider (CSP)	<ul style="list-style-type: none">• Commercial vendor or Federal organization offering or providing cloud services (Includes DoD CSPs)• Provides Cloud Service Offerings• Provides CNDSP services (all tiers) for their infrastructure and service offerings
FedRAMP Joint Authorization Board (JAB)	<ul style="list-style-type: none">• Reviews CSP security assessment packages• Grants FedRAMP Provisional Authorizations
Third Party Assessment Organizations (3PAO)	<ul style="list-style-type: none">• Independently performs security assessments of CSP the organization and systems and creates security assessment package artifacts in accordance with FedRAMP requirements• May perform continuous monitoring of CSP systems• May also assess DoD FedRAMP+ security controls

DRAFT

Role	Responsibility
DoD Cloud Service Broker	<p>Per DoD CIO Memo</p> <ul style="list-style-type: none"> • Provide security requirements guidelines (SRGs) and Security Technical Implementation Guidance (STIGs) for DoD cloud computing. (DISA FSO) • Issue DoD Provisional Authorizations. (DISA AO) • Provide clear instructions to industry and the Components on DoD cybersecurity requirements. • Develop and maintain a DoD Cloud Access Point (CAP). • Provide DoDIN Computer Network Defense (CND) capabilities and maintain a CND concept of operations (CONOPS). • Provide technical support for the DoD CIO's role on the FedRAMP Joint Authorization Board. (DISA FSO) • Provide a catalog of DoD cloud services. • Maintain a registry of DoD Components using commercial cloud services. • Support the DoDIN Waiver Process. • Recommend policy and guidance updates. • Advance Cloud Broker Functions (maintain and enhance the Cloud Broker role) • Receives CSP's continuous monitoring products and passes them to the appropriate entities within DoD • Certifier for CSP's Service Offerings receiving PA from the DISA AO and consumer of CNDSP information.
DISA Authorizing Official (AO)	<ul style="list-style-type: none"> • Official approving PA for a CSP's Service Offerings for DoD use
DoD Component Authorizing Official (AO)	<ul style="list-style-type: none"> • Official approving ATOs for Mission Owner's systems/applications • Reviews PA documentation to understand residual risk
DISA Field Security Operations (FSO)	<ul style="list-style-type: none"> • Reviews/assesses CSP's continuous monitoring products • Assists the FedRAMP Technical Representative for DoD's JAB representative • Developer and maintainer of SRGs and STIGs • Coordinates the DISA CNDSP program for DISA and others
DISA DoDIN Readiness and Security Inspections (DRSI)	<ul style="list-style-type: none"> • DoD CNDSP certifier

Role	Responsibility
<p>Mission Owner (CSP's DoD Cloud Customer DoD Cloud Consumer)</p>	<ul style="list-style-type: none"> • DoD entity that acquires cloud services in support of its mission • Performs assessment to issue ATO for their mission systems/applications • Ensures Tier 2 Mission Computer Network Defense (MCND) Service Provider is identified and funded • Serves as CND Tier 3 for their mission systems/applications
<p>Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT)</p>	<ul style="list-style-type: none"> • Receives incident reports from CSP as mandated by FedRAMP. • Responsible for coordination across non-DoD agencies
<p>Computer Network Defense Service Provider (CNDSP)</p>	<ul style="list-style-type: none"> • Provides Computer Network Defense (CND) services and Command and Control (C2) direction addressing the protection of the network, detection of threats, and response to incidents.
<p>United States Cyber Command (USCYBERCOM)</p> <ul style="list-style-type: none"> • DoD Tier 1 CNDSP 	<ul style="list-style-type: none"> • Notify and Coordinate as appropriate with US-CERT, Intelligence Community, Law Enforcement, and other Federal Agencies • Provides Computer Network Defense (CND) services and Command and Control (C2) direction for the entire DoDIN and all DoD information systems
<p>Boundary CND (BCND)</p> <ul style="list-style-type: none"> • DoD Tier 2 CNDSP 	<ul style="list-style-type: none"> • Monitors and defends the connections to/from off-premises CSPs at the Cloud Access Point (CAP) • Provides cross-CSP analysis capabilities or entities • Serves as the DoD CND / C2 point of contact for the CSP • Communicates with CND Tier 1 and Tier 2 entities
<p>Mission CND (MCND)</p> <ul style="list-style-type: none"> • DoD Tier 2 CNDSP 	<ul style="list-style-type: none"> • Provides CND / C2 services to specific Mission Owner's systems/applications and virtual networks • Communicates with CND Tier 2 and Tier 3 entities

Appendix D Parameter Values

Table 9 provides a listing of the FedRAMP and FedRAMP+ controls / control enhancements that require values and the DoD specified Parameter Values for them. Both DoD RMF and FedRAMP values are provided along with the FedRAMP Additional Requirements and Guidance. These are provided in the format used by the originator. The purpose is to provide a comparison between the DoD and FedRAMP values and to provide the FedRAMP Additional Requirements and Guidance for use by DoD assessors and CSPs. All CSPs are to be assessed IAW the same set of Cs/CEs and values. For all CSPs, the DoD RMF value takes precedence unless the FedRAMP value is more stringent. The full control / control enhancement text is included to provide full context for the value being addressed.

NOTE: For parameter values tagged as “Not appropriate for DoD to define for all CSP's infrastructure or service offerings.” The CSP must provide details on how this control / control enhancement is met to include it's values in the SSP for the DoD AO to approve.

Table 9 – Control / Enhancement Parameter Values

Control/Enhancement text	Value
<p>AC-1; ACCESS CONTROL; Access Control Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency]. <p>References: NIST Special Publications 800-12, 800-100.</p>	<p>AC-1</p> <ol style="list-style-type: none"> a. all personnel b. Annually <p>Source: DoD RMF TAG -----</p> <p>AC-1.b.1 [at least every 3 years] AC-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>AC-2; ACCESS CONTROL; Account Management:</p> <p>The organization:</p> <p>a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];</p> <p>b. Assigns account managers for information system accounts;</p> <p>c. Establishes conditions for group and role membership;</p> <p>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;</p> <p>e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;</p> <p>f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];</p> <p>g. Monitors the use of, information system accounts;</p> <p>h. Notifies account managers:</p> <ol style="list-style-type: none"> 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; <p>i. Authorizes access to the information system based on:</p> <ol style="list-style-type: none"> 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; <p>j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and</p> <p>k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.</p> <p>References: None.</p>	<p>AC-2</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>e. ISSM or ISSO</p> <p>f. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>j. at a minimum, annually</p> <p>Source: DoD RMF TAG -----</p> <p>AC-2j [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>AC-2 (2); ACCESS CONTROL; Account Management - Enhancement: Removal Of Temporary Emergency Accounts</p> <p>The information system automatically [Selection: - removes; - disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].</p> <p>References: None.</p>	<p>AC-2 (2) For temporary user accounts: 72 hours</p> <p>For emergency admin accounts: never (see supplemental recommendation)</p> <p>Source: DoD RMF TAG -----</p> <p>[No more than 30 days for temporary and emergency account types]</p> <p>Source: FedRAMP v2 -----</p>

<p>AC-2 (3); ACCESS CONTROL; Account Management - Enhancement: Disable Inactive Accounts</p> <p>The information system automatically disables inactive accounts after [Assignment: organization-defined time period].</p> <p>References: None.</p>	<p>AC-2 (3) 35 days</p> <p>Source: DoD RMF TAG -----</p> <p>[90 days for user accounts]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Authorizing Official.</p>
<p>AC-2 (4); ACCESS CONTROL; Account Management - Enhancement: Automated Audit Actions</p> <p>The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>AC-2 (4) System administrator and ISSO</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-2 (5); ACCESS CONTROL; Account Management - Enhancement: Inactivity Logout</p> <p>The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].</p> <p>References: None.</p>	<p>AC-2 (5) At the end of the users standard work period unless otherwise defined in formal organizational policy.</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-2 (7); ACCESS CONTROL; Account Management - Enhancement: Role-Based Schemes</p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. <p>References: None.</p>	<p>AC-2 (7) c. Disables (or revokes) privileged user account</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-2 (9); ACCESS CONTROL; Account Management - Enhancement: Restrictions On Use Of Shared Groups / Accounts</p> <p>The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].</p> <p>References: None.</p>	<p>AC-2 (9) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: Required if shared/group accounts are deployed</p>

<p>AC-2 (12); ACCESS CONTROL; Account Management - Enhancement: Account Monitoring /Atypical Usage</p> <p>The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]; and (b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>AC-2 (12) a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings b. at a minimum, the ISSO</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: AC-2 (12)(a) and AC-2 (12)(b) Additional FedRAMP Requirements and Guidance: Required for privileged accounts.</p>
<p>AC-2 (13); ACCESS CONTROL; Account Management - Enhancement: Disable Accounts For High-Risk Individuals</p> <p>The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.</p> <p>References: None.</p>	<p>AC-2 (13) 30 minutes unless otherwise defined in formal organizational policy</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-3 (4); ACCESS CONTROL; Access Enforcement - Enhancement: Discretionary Access Control</p> <p>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.</p> <p>References: None.</p>	<p>AC-3 (4) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-4; ACCESS CONTROL; Information Flow Enforcement:</p> <p>The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].</p> <p>References: Web: ucdmo.gov</p>	<p>AC-4 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-4 (21); ACCESS CONTROL; Information Flow Enforcement - Enhancement: Physical / Logical Separation Of Information Flows</p> <p>The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].</p> <p>References: None.</p>	<p>AC-4 (21) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>AC-5; ACCESS CONTROL; Separation Of Duties:</p> <p>The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.</p> <p>References: None.</p>	<p>AC-5 a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-6 (1); ACCESS CONTROL; Least Privilege - Enhancement: Authorize Access To Security Functions</p> <p>The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].</p> <p>References: None.</p>	<p>AC-6 (1) all functions not publicly accessible and all security-relevant information not publicly available</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-6 (2); ACCESS CONTROL; Least Privilege - Enhancement: Non-Privileged Access For Nonsecurity Functions</p> <p>The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts, or roles, when accessing nonsecurity functions.</p> <p>References: None.</p>	<p>AC-6 (2) any privileged security functions or security-relevant information</p> <p>Source: DoD RMF TAG -----</p> <p>[all security functions]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: AC-6 (2). Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.</p>
<p>AC-6 (5); ACCESS CONTROL; Least Privilege - Enhancement: Privileged Accounts</p> <p>The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>AC-6 (5) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-6 (7); ACCESS CONTROL; Least Privilege - Enhancement: Review Of User Privileges</p> <p>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.</p> <p>References: None.</p>	<p>AC-6 (7) a. at a minimum, annually</p> <p>a. all users</p> <p>Source: DoD RMF TAG -----</p>

<p>AC-6 (8); ACCESS CONTROL; Least Privilege - Enhancement: Privilege Levels For Code Execution</p> <p>The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.</p> <p>References: None.</p>	<p>AC-6 (8) any software except software explicitly documented</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-7; ACCESS CONTROL; Unsuccessful Login Attempts:</p> <p>The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid login attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: - locks the account/node for an [Assignment: organization-defined time period]; - locks the account/node until released by an administrator; - delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.</p> <p>References: None.</p>	<p>AC-7 a(1). Three a(2). 15 minutes b(1). locks the account/node b(2). Until released by an administrator b(3). Minimum of 5 seconds</p> <p>Source: DoD RMF TAG -----</p> <p>AC-7a [not more than three] [fifteen minutes]</p> <p>AC-7b [locks the account/node for thirty minutes]</p> <p>Source: FedRAMP v2 -----</p>
<p>AC-8; ACCESS CONTROL; System Use Notification:</p> <p>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.</p> <p>References: None.</p>	<p>AC-8 a. The content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013</p> <p>c. The content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013</p> <p>Source: DoD RMF TAG -----</p> <p>Parameter: See Additional Requirements and Guidance.</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Authorizing Official (AO). Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the AO. Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided. Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the AO.</p>

<p>AC-10; ACCESS CONTROL; Concurrent Session Control:</p> <p>The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].</p> <p>References: None.</p>	<p>AC-10 all account types and/or accounts</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>[three (3) sessions for privileged access and two (2) sessions for non-privileged access]</p> <p>Source: FedRAMP v2 -----</p>
<p>AC-11; ACCESS CONTROL; Session Lock:</p> <p>The information system:</p> <p>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</p> <p>b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.</p> <p>References: OMB Memorandum 06-16.</p>	<p>AC-11 a. 15 minutes</p> <p>Source: DoD RMF TAG -----</p> <p>AC-11a. [fifteen minutes]</p> <p>Source: FedRAMP v2 -----</p>
<p>AC-12; ACCESS CONTROL; Session Termination:</p> <p>The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].</p> <p>References: None.</p>	<p>AC-12 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-12 (1); ACCESS CONTROL; Session Termination - Enhancement: User-Initiated Logouts / Message Displays</p> <p>The information system:</p> <p>(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and</p> <p>(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.</p> <p>References: None.</p>	<p>AC-12 (1) a. all</p> <p>Source: DoD RMF TAG -----</p>

<p>AC-14; ACCESS CONTROL; Permitted Actions Without Identification Or Authentication:</p> <p>The organization:</p> <p>a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.</p> <p>References: None.</p>	<p>AC-14 a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-16; ACCESS CONTROL; Security Attributes:</p> <p>The organization:</p> <p>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.</p> <p>References: None.</p>	<p>AC-16 a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>c. security attributes defined in AC-16, CCI's 2256-2258</p> <p>c. all information systems</p> <p>d. the values defined in AC-16, CCI's 2259-2261</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-16 (6); ACCESS CONTROL; Security Attributes - Enhancement: Maintenance Of Attribute Association By Organization</p> <p>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].</p> <p>References: None.</p>	<p>AC-16 (6) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-17 (3); ACCESS CONTROL; Remote Access - Enhancement: Managed Access Control Points</p> <p>The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.</p> <p>References: None.</p>	<p>AC-17 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>AC-17 (4); ACCESS CONTROL; Remote Access - Enhancement: Privileged Commands / Access</p> <p>The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system.</p> <p>References: None.</p>	<p>AC-17 (4) a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-17 (9); ACCESS CONTROL; Remote Access - Enhancement: Disconnect / Disable Access</p> <p>The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [Assignment: organization-defined time period].</p> <p>References: None.</p>	<p>AC-17 (9) immediately</p> <p>Source: DoD RMF TAG -----</p> <p>[no greater than 15 minutes]</p> <p>Source: FedRAMP v2 -----</p>
<p>AC-19 (5); ACCESS CONTROL; Access Control For Mobile Devices - Enhancement: Full Device / Container- Based Encryption</p> <p>The organization employs [Selection: - full-device encryption; - container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].</p> <p>References: None.</p>	<p>AC-19 (5) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AC-21; ACCESS CONTROL; User-Based Collaboration And Information Sharing RENAMED: Information Sharing:</p> <p>The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.</p> <p>References: None.</p>	<p>AC-21 a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

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

<p>AT-3; AWARENESS AND TRAINING ; Security Training RENAMED: Role-based Security Training:</p> <p>The organization provides role-based security training to personnel with assigned security roles and responsibilities:</p> <ol style="list-style-type: none"> Before authorizing access to the information system or performing assigned duties; When required by information system changes; and [Assignment: organization-defined frequency] thereafter. <p>References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publications 800-16, 800-50.</p>	<p>AT-3 c. annually</p> <p>Source: DoD RMF TAG -----</p> <p>AT-3c. [Assignment: organization-defined frequency]</p> <p>Parameter: [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>AT-3 (2); AWARENESS AND TRAINING ; Security Training RENAMED: Role-based Security Training - Enhancement: Physical Security Controls</p> <p>The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.</p> <p>References: None.</p>	<p>AT-3 (2) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Annual</p> <p>Source: DoD RMF TAG -----</p>
<p>AT-3 (4); AWARENESS AND TRAINING; Role-based Security Training - Enhancement: Suspicious Communications And Anomalous System Behavior</p> <p>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.</p> <p>References: None.</p>	<p>AT-3 (4) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AT-4; AWARENESS AND TRAINING ; Security Training Records:</p> <p>The organization:</p> <ol style="list-style-type: none"> Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and Retains individual training records for [Assignment: organization-defined time period]. <p>References: None.</p>	<p>AT-4 b. at least 5 years or 5 years after completion of a specific training program</p> <p>Source: DoD RMF TAG -----</p> <p>AT-4b. [Assignment: organization-defined frequency]</p> <p>Parameter: [At least one years]</p> <p>Source: FedRAMP v2 -----</p>

<p>AU-1; AUDIT AND ACCOUNTABILITY; Audit And Accountability Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none">1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; <p>and</p> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none">1. Audit and accountability policy [Assignment: organization-defined frequency]; <p>and</p> <ol style="list-style-type: none">2. Audit and accountability procedures [Assignment: organization-defined frequency]. <p>References: NIST Special Publications 800-12, 800-100.</p>	<p>AU-1</p> <p>a. the ISSO and ISSM and others as the local organization deems appropriate</p> <p>b. 1. Annually b. 2. Annually</p> <p>Source: DoD RMF TAG -----</p> <p>AU-1.b.1 [at least every 3 years] AU-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>AU-2; AUDIT AND ACCOUNTABILITY; Auditable Events:</p> <p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>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;</p> <p>c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and</p> <p>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].</p> <p>References: NIST Special Publication 800-92; Web: CSRC.NIST.GOV/PCIG/CIG.HTML, IDMANAGEMENT.GOV</p>	<p>AU-2</p> <p>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.</p> <p>d. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>d. all auditable events defined in AU-2 (a) per occurrence.</p> <p>Source: DoD RMF TAG -----</p> <p>AU-2a. [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes];</p> <p>AU-2d. [organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event].</p> <p>Source: FedRAMP v2 -----</p>

<p>AU-2 (3); AUDIT AND ACCOUNTABILITY; Auditable Events - Enhancement: Reviews And Updates</p> <p>The organization reviews and updates the audited events [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>AU-2 (3) Annually and based on situational awareness of threats, vulnerabilities</p> <p>Source: DoD RMF TAG -----</p> <p>AU-2 (3). [Assignment: organization-defined frequency]</p> <p>Parameter: [annually or whenever there is a change in the threat environment]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the Authorizing Official.</p>
<p>AU-3 (1); AUDIT AND ACCOUNTABILITY; Content Of Audit Records - Enhancement: Additional Audit Information</p> <p>The information system generates audit records containing the following [Assignment: organization-defined additional, more detailed information].</p> <p>References: None.</p>	<p>AU-3 (1) At a minimum, full-text recording of privileged commands or the individual identities of group account users.</p> <p>Source: DoD RMF TAG -----</p> <p>AU-3 (1). [Assignment: organization-defined additional, more detailed information] Parameter: [session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: AU-3 (1). Requirement: The service provider defines audit record types. The audit record types are approved and accepted by the Authorizing Official. Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.</p>
<p>AU-4; AUDIT AND ACCOUNTABILITY; Audit Storage Capacity:</p> <p>The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].</p> <p>References: None.</p>	<p>AU-4 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AU-4 (1); AUDIT AND ACCOUNTABILITY; Audit Storage Capacity - Enhancement: Transfer To Alternate Storage</p> <p>The information system off-loads audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.</p> <p>References: None.</p>	<p>AU-4 (1) At a minimum, real-time for interconnected systems and weekly for stand-alone systems</p> <p>Source: DoD RMF TAG -----</p>

<p>AU-5; AUDIT AND ACCOUNTABILITY; Response To Audit Processing Failures:</p> <p>The information system:</p> <p>a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and</p> <p>b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].</p> <p>References: None.</p>	<p>AU-5</p> <p>a. At a minimum, the SCA and ISSO</p> <p>b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>AU-5b. [Assignment: Organization-defined actions to be taken]</p> <p>Parameter: [low-impact: overwrite oldest audit records; moderate-impact: shut down]</p> <p>Source: FedRAMP v2 -----</p>
<p>AU-6; AUDIT AND ACCOUNTABILITY; Audit Review, Analysis, And Reporting:</p> <p>The organization:</p> <p>a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and</p> <p>b. Reports findings to [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>AU-6</p> <p>a. every seven days or more frequently if required by an alarm event or anomaly;</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>b. at a minimum, the ISSO and ISSM</p> <p>Source: DoD RMF TAG -----</p> <p>AU-6a. [Assignment: organization-defined frequency]</p> <p>Parameter: [at least weekly]</p> <p>Source: FedRAMP v2 -----</p>
<p>AU-7 (1); AUDIT AND ACCOUNTABILITY; Audit Reduction And Report Generation - Enhancement: Automatic Processing</p> <p>The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].</p> <p>References: None.</p>	<p>AU-7 (1)</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AU-8; AUDIT AND ACCOUNTABILITY; Time Stamps:</p> <p>The information system:</p> <p>a. Uses internal system clocks to generate time stamps for audit records; and</p> <p>b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].</p> <p>References: None.</p>	<p>AU-8</p> <p>b. one second</p> <p>Source: DoD RMF TAG -----</p>

<p>AU-8 (1); AUDIT AND ACCOUNTABILITY; Protection Of Audit Information - Enhancement: Synchronization With Authoritative Time Source</p> <p>The information system: a. Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source] and; b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].</p> <p>References: None.</p>	<p>AU-8 (1) a. Every 24 hours for networked systems; a. an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS); b. Greater than the organizationally defined granularity in AU-8</p> <p>Source: DoD RMF TAG -----</p> <p>AU-8 (1). [http://tf.nist.gov/tf-cgi/servers.cgi] <At least hourly></p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: AU-8 (1). Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server. Guidance: Synchronization of system clocks improves the accuracy of log analysis.</p>
<p>AU-9 (2); AUDIT AND ACCOUNTABILITY; Protection Of Audit Information - Enhancement: Audit Backup On Separate Physical Systems / Components</p> <p>The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited.</p> <p>References: None.</p>	<p>AU-9 (2) every seven days</p> <p>Source: DoD RMF TAG -----</p> <p>AU-9 (2). [at least weekly]</p> <p>Source: FedRAMP v2 -----</p>
<p>AU-9 (4); AUDIT AND ACCOUNTABILITY; Protection Of Audit Information - Enhancement: Access By Subset Of Privileged Users</p> <p>The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].</p> <p>References: None.</p>	<p>AU-9 (4) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>AU-10; AUDIT AND ACCOUNTABILITY; Non-Repudiation:</p> <p>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].</p> <p>References: None.</p>	<p>AU-10 actions defined by DoDI 8520.02 and DoDI 8520.03</p> <p>Source: DoD RMF TAG -----</p>

<p>AU-11; AUDIT AND ACCOUNTABILITY; Audit Record Retention:</p> <p>The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</p> <p>References: None.</p>	<p>AU-11 5 years for SAMI; otherwise for at least 1 year</p> <p>Source: DoD RMF TAG -----</p> <p>AU-11. [at least ninety days]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: AU-11. Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.</p>
<p>AU-12; AUDIT AND ACCOUNTABILITY; Audit Generation:</p> <p>The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.</p> <p>References: None.</p>	<p>AU-12 a. all information system and network components; b. ISSM or individuals appointed by the ISSM</p> <p>Source: DoD RMF TAG -----</p> <p>AU-12a. [all information system and network components where audit capability is deployed/available]</p> <p>Source: FedRAMP v2 -----</p>
<p>AU-12 (1); AUDIT AND ACCOUNTABILITY; Audit Generation - Enhancement: System-Wide / Time-Correlated Audit Trail</p> <p>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].</p> <p>References: None.</p>	<p>AU-12 (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>The time tracking tolerance defined in AU-8</p> <p>Source: DoD RMF TAG -----</p>
<p>AU-12 (3); AUDIT AND ACCOUNTABILITY; Audit Generation - Enhancement: Changes By Authorized Individuals</p> <p>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].</p> <p>References: None.</p>	<p>AU-12 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>Source: DoD RMF TAG -----</p>

<p>CA-1; SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessment And Authorization Policies And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls;</p> <p>and</p> <p>b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency].</p> <p>References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.</p>	<p>CA-1 a. all personnel</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>CA-1.b.1 [at least every 3 years] CA-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>CA-2; SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments:</p> <p>The organization:</p> <p>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;</p> <p>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;</p> <p>c. Produces a security assessment report that documents the results of the assessment; and</p> <p>d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].</p> <p>References: Executive Order 12587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137</p>	<p>CA-2 b. Annually for technical controls Annually for a portion of management and operational controls such that all are reviewed in a 3 year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1.</p> <p>d. at a minimum, the ISSO and ISSM</p> <p>Source: DoD RMF TAG -----</p> <p>CA-2b. [at least annually] CA-2d[individuals or roles to include FedRAMP PMO]</p> <p>Source: FedRAMP v2 -----</p>
<p>CA-2 (1); SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments - Enhancement: Independent Assessors</p> <p>The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.</p> <p>References: None.</p>	<p>CA-2 (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>Added to NIST Baseline for "Low" FedRAMP baseline.</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: For JAB Authorization, must be an accredited 3PAO</p>

<p>CA-2 (2); SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments - Enhancement: Specialized Assessments</p> <p>The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: <ul style="list-style-type: none"> - announced; - unannounced], [Selection (one or more): <ul style="list-style-type: none"> - in-depth monitoring; - vulnerability scanning; - malicious user testing; - insider threat assessment; - performance/load testing; - [Assignment: organization-defined other forms of security assessment]].</p> <p>References: None.</p>	<p>CA-2 (2) annually</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>[at least annually]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Requirement: To include 'announced', 'vulnerability scanning'</p>
<p>CA-2 (3); SECURITY ASSESSMENT AND AUTHORIZATION; Security Assessments - Enhancement: External Organizations</p> <p>The organization accepts the results of an assessment of [Assignment: organization-defined information system] performed by [Assignment: organization-defined external organization] when the assessment meets [Assignment: organization-defined requirements].</p> <p>References: None.</p>	<p>CA-2 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>[Any FedRAMP Accredited 3PAO] [the conditions of a P-ATO in the FedRAMP Repository]</p> <p>Source: FedRAMP v2 -----</p>
<p>CA-3; SECURITY ASSESSMENT AND AUTHORIZATION; Information System Connections RENAMED: System Interconnections:</p> <p>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].</p> <p>References: FIPS Publication 199; NIST Special Publication 800-47.</p>	<p>CA-3 c. at least annually</p> <p>Source: DoD RMF TAG -----</p> <p>CA-3c. 3 Years / Annually and on input from FedRAMP</p> <p>Source: FedRAMP v2 -----</p>

<p>CA-3 (1); SECURITY ASSESSMENT AND AUTHORIZATION; Information System Connections RENAME: System Interconnections - Enhancement: Unclassified National Security System Connections</p> <p>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].</p> <p>References: None.</p>	<p>CA-3 (1) all unclassified NSS</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>CA-3 (3); SECURITY ASSESSMENT AND AUTHORIZATION; System Interconnections - Enhancement: Unclassified Non-National Security System Connections</p> <p>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].</p> <p>References: None.</p>	<p>CA-3 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>Boundary Protections which meet the Trusted Internet Connection (TIC) requirements</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: CA-3(3) Guidance: Refer to Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document.</p>
<p>CA-3 (5); SECURITY ASSESSMENT AND AUTHORIZATION; System Interconnections - Enhancement: Restrictions On External System Connections</p> <p>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.</p> <p>References: None.</p>	<p>CA-3 (5) deny-all, permit by exception</p> <p>any systems requiring external connectivity</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing</p>

<p>CA-5; SECURITY ASSESSMENT AND AUTHORIZATION; Plan Of Action And Milestones:</p> <p>The organization:</p> <p>a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and</p> <p>b. Updates existing plan of action and milestones [Assignment: organization-defined frequency]</p> <p>based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.</p> <p>References: OMB Memorandum 02-01; NIST Special Publication 800-37.</p>	<p>CA-5 b. At least every 90 days</p> <p>Source: DoD RMF TAG -----</p> <p>CA-5b. [at least monthly]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: CA-5 Guidance: Requirement: POA&Ms must be provided at least monthly.</p>
<p>CA-6; SECURITY ASSESSMENT AND AUTHORIZATION; Security Authorization:</p> <p>The organization:</p> <p>a. Assigns a senior-level executive or manager as the authorizing official for the information system;</p> <p>b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and</p> <p>c. Updates the security authorization [Assignment: organization-defined frequency].</p> <p>References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publication 800-37, 800-137.</p>	<p>CA-6 c. at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.</p> <p>Source: DoD RMF TAG -----</p> <p>CA-6c. [at least every three years or when a significant change occurs]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: CA-6c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the Authorizing Official.</p>
<p>CA-7; SECURITY ASSESSMENT AND AUTHORIZATION; Continuous Monitoring:</p> <p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <p>a. Establishment of [Assignment: organization-defined metrics]</p> <p>to be monitored;</p> <p>b. Establishment of [Assignment: organization-defined frequencies]</p> <p>for monitoring and [Assignment: organization-defined frequencies]</p> <p>for assessments supporting such monitoring;</p> <p>c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;</p> <p>d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;</p> <p>e. Correlation and analysis of security-related information generated by assessments and monitoring;</p> <p>f. Response actions to address results of the analysis of security-related information; and</p> <p>g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].</p> <p>References: OMB Memorandum 11-33; NIST Special Publications 800-37 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DOD Information Assurance Vulnerability Alerts.</p>	<p>CA-7 Future DoD-wide CM guidance to be published.</p> <p>Source: DoD RMF TAG -----</p> <p>CA-7d. [To meet Federal and FedRAMP requirements]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Operating System Scans: at least monthly Database and Web Application Scans: at least monthly All scans performed by Independent Assessor: at least annually</p> <p>CA-7 Guidance: CSPs must provide evidence of closure and remediation of high vulnerabilities within the timeframe for standard POA&M updates.</p>

<p>CA-7 (1); SECURITY ASSESSMENT AND AUTHORIZATION; Continuous Monitoring - Enhancement: Independent Assessment</p> <p>The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.</p> <p>References: None.</p>	<p>CA-7 (1) Future DoD-wide CM guidance to be published.</p> <p>Source: DoD RMF TAG -----</p>
<p>CA-8; SECURITY ASSESSMENT AND AUTHORIZATION; Penetration Testing:</p> <p>The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].</p> <p>References: None.</p>	<p>CA-8 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>[at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>CA-9; SECURITY ASSESSMENT AND AUTHORIZATION; Internal System Connections:</p> <p>The organization:</p> <p>a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and</p> <p>b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.</p> <p>References: None.</p>	<p>CA-9 a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>CM-1; BASELINE CONFIGURATION; Configuration Management Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls;</p> <p>and</p> <p>b. Reviews and updates the current:</p> <p>1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency].</p> <p>References: NIST Special Publications 800-12, 800-100.</p>	<p>CM-1 a. all stakeholders in the configuration management process b. 1. annually b. 2. annually</p> <p>Source: DoD RMF TAG -----</p> <p>CM-1.b.1 [at least every 3 years] CM-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>CM-2 (1); BASELINE CONFIGURATION; Baseline Configuration - Enhancement: Reviews And Updates</p> <p>The organization reviews and updates the baseline configuration of the information system:</p> <p>(a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades.</p> <p>References: None.</p>	<p>CM-2 (1) a. annually; b. baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.</p> <p>Source: DoD RMF TAG -----</p> <p>CM-2 (1) (a). [at least annually] CM-2 (1) (b). [to include when directed by Authorizing Official]</p> <p>Source: FedRAMP v2 -----</p>
<p>CM-2 (3); BASELINE CONFIGURATION; Baseline Configuration - Enhancement: Retention Of Previous Configurations</p> <p>The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.</p> <p>References: None.</p>	<p>CM-2 (3) the previous approved baseline configuration of IS components for a minimum of 3 month</p> <p>Source: DoD RMF TAG -----</p>
<p>CM-2 (7); CONFIGURATION MANAGEMENT; Baseline Configuration - Enhancement: Configure Systems, Components, Or Devices For High-Risk Areas</p> <p>The organization:</p> <p>a. Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and</p> <p>b. Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.</p> <p>References: None.</p>	<p>CM-2 (7) a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings; a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings; b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>CM-3; BASELINE CONFIGURATION; Configuration Change Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Determines the type of changes to the information system that are configuration controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through <p>[Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes</p> <p>[Selection (one or more):</p> <ul style="list-style-type: none"> - [Assignment: organization-defined frequency]; - [Assignment: organization-defined configuration change conditions] <p>].</p> <p>References: NIST Special Publication 800-128.</p>	<p>CM-3</p> <ul style="list-style-type: none"> e. The time period should be defined at the organization's CCB. g. a configuration control board; g. at a frequency determined by the CCB; g. configuration change conditions determined by the CCB. <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the Authorizing Official.</p> <p>CM-3e Guidance: In accordance with record retention policies and procedures.</p>
<p>CM-3 (4); BASELINE CONFIGURATION; Configuration Change Control - Enhancement: Security Representative</p> <p>The organization requires an information security representative to be a member of the</p> <p>[Assignment: organization-defined configuration change control element].</p> <p>References: None.</p>	<p>CM-3 (4) configuration control board (CCB) (as defined in CM-3, CCI 1586)</p> <p>Source: DoD RMF TAG -----</p>
<p>CM-3 (6); CONFIGURATION MANAGEMENT; Configuration Change Control - Enhancement: Cryptography Management</p> <p>The organization ensures that cryptographic mechanisms used to provide</p> <p>[Assignment: organization-defined security safeguards] are under configuration management.</p> <p>References: None.</p>	<p>CM-3 (6) All security safeguards that rely on cryptography</p> <p>Source: DoD RMF TAG CNSSI 1253</p>
<p>CM-5 (2); BASELINE CONFIGURATION; Access Restrictions For Change - Enhancement: Review System Changes</p> <p>The organization reviews information system changes</p> <p>[Assignment: organization-defined frequency] and</p> <p>[Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.</p> <p>References: None.</p>	<p>CM-5 (2) Every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems;</p> <p>When there is an incident or when planned changes have been performed</p> <p>Source: DoD RMF TAG -----</p>

<p>CM-5 (3); BASELINE CONFIGURATION; Access Restrictions For Change - Enhancement: Signed Components</p> <p>The information system prevents the installation of [Assignment: organization-defined critical software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.</p> <p>References: None.</p>	<p>CM-5 (3) Any software or firmware components when the vendor provides digitally signed products</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized.</p>
<p>CM-5 (5); BASELINE CONFIGURATION; Access Restrictions For Change - Enhancement: Limit Production / Operational Privileges</p> <p>The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>CM-5 (5) b. every 90 days</p> <p>Source: DoD RMF TAG -----</p> <p>CM-5 (5) (b). [at least quarterly]</p> <p>Source: FedRAMP v2 -----</p>
<p>CM-6; BASELINE CONFIGURATION; Configuration Settings:</p> <p>The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.</p> <p>References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov; checklists.nist.gov; www.nsa.gov.</p>	<p>CM-6 a. DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.); c. All configurable information system components; c. Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>Source: DoD RMF TAG -----</p> <p>CM-6a. [See CM-6(a) Additional FedRAMP Requirements and Guidance]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: CM-6a. Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. CM-6a. Requirement: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). CM-6a. Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc .</p>
<p>CM-6 (1); BASELINE CONFIGURATION; Configuration Settings - Enhancement: Automated Central Management / Application / Verification</p> <p>The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].</p> <p>References: None.</p>	<p>CM-6 (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>CM-7; BASELINE CONFIGURATION; Least Functionality:</p> <p>The organization:</p> <p>a. Configures the information system to provide only essential capabilities; and</p> <p>b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services:</p> <p>[Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].</p> <p>References: DoD Instruction 8551.01</p>	<p>CM-7 IAW DoDI 8551.01</p> <p>Source: DoD RMF TAG -----</p> <p>CM-7. [United States Government Configuration Baseline (USGCB)]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. CM-7. Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc. (Partially derived from AC-17(8).)</p>
<p>CM-7 (1); BASELINE CONFIGURATION; Least Functionality - Enhancement: Periodic Review</p> <p>The organization:</p> <p>a. Reviews the information system</p> <p>[Assignment: organization-defined frequency]</p> <p>to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and</p> <p>b. Disables</p> <p>[Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].</p> <p>References: None.</p>	<p>CM-7 (1) a. every 30 days; b. Not appropriate to define unnecessary functions, ports, protocols and service at the Enterprise level. Nonsecure functions, ports, protocols and services are defined in DoDI 8551.01.</p> <p>Source: DoD RMF TAG -----</p> <p>CM-7(1) [At least Monthly]</p> <p>Source: FedRAMP v2 -----</p>
<p>CM-7 (2); BASELINE CONFIGURATION; Least Functionality - Enhancement: Prevent Program Execution</p> <p>The information system prevents program execution in accordance with</p> <p>[Selection (one or more):</p> <ul style="list-style-type: none"> - [Assignment: organization-defined policies regarding software program usage and restrictions]; - rules authorizing the terms and conditions of software program usage]. <p>References: None.</p>	<p>CM-7 (2) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: CM-7(2) Guidance: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e. white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.</p>

<p>CM-7 (5); CONFIGURATION MANAGEMENT; Least Functionality - Enhancement: Authorized Software / Whitelisting</p> <p>The organization: a. Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and c. Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>CM-7 (5) a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings; c. Monthly</p> <p>Source: DoD RMF TAG -----</p> <p>CM-7(5)[at least Annually or when there is a change.]</p> <p>Source: FedRAMP v2 -----</p>
<p>CM-8; BASELINE CONFIGURATION; Information System Component Inventory:</p> <p>The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].</p> <p>References: NIST Special Publication 800-128.</p>	<p>CM-8 a. hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.; b. at a minimum, annually</p> <p>Source: DoD RMF TAG -----</p> <p>CM-8b. [at least monthly]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: CM-8 Requirement: must be provided at least monthly or when there is a change.</p>
<p>CM-8 (3); BASELINE CONFIGURATION; Information System Component Inventory - Enhancement: Automated Unauthorized Component Detection</p> <p>The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): - disables network access by such components; - isolates the components; - notifies [Assignment: organization-defined personnel or roles]].</p> <p>References: None.</p>	<p>CM-8 (3) a. continuously; b. the ISSO and ISSM and others as the local organization deems appropriate</p> <p>Source: DoD RMF TAG -----</p> <p>CM-8 (3) (a). [Continuously, using automated mechanisms with a maximum five-minute delay in detection.]</p> <p>Source: FedRAMP v2 -----</p>
<p>CM-10 (1); CONFIGURATION MANAGEMENT; Software Usage Restrictions - Enhancement: Open Source Software</p> <p>The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].</p> <p>References: None.</p>	<p>CM-10 (1) IAW DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx).</p> <p>Source: DoD RMF TAG -----</p>

<p>CM-11; CONFIGURATION MANAGEMENT; User-Installed Software:</p> <p>The organization:</p> <p>a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;</p> <p>b. Enforces software installation policies through [Assignment: organization-defined methods]; and</p> <p>c. Monitors policy compliance at [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>CM-11</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings;</p> <p>c. at least monthly</p> <p>Source: DoD RMF TAG -----</p> <p>CM-11.c. [Continuously (via CM-7 (5))]</p> <p>Source: FedRAMP v2 -----</p>
<p>CP-1; CONTINGENCY PLANNING; Contingency Planning Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <p>1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls;</p> <p>and</p> <p>b. Reviews and updates the current:</p> <p>1. Contingency planning policy [Assignment: organization-defined frequency]; and</p> <p>2. Contingency planning procedures [Assignment: organization-defined frequency].</p> <p>References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.</p>	<p>CP-1</p> <p>a. all stakeholders identified in the contingency plan</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>CP-1.b.1 [at least every 3 years] CP-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

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

<p>CP-4; CONTINGENCY PLANNING; Contingency Plan Testing And Exercises RENAMED: Contingency Plan Testing:</p> <p>The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.</p> <p>References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.</p>	<p>CP-4 a. at least annually</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>CP-4a. [at least annually for moderate impact systems; at least every three years for low impact systems] [functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: CP-4a. Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by the Authorizing Official prior to initiating testing.</p>
<p>CP-7; CONTINGENCY PLANNING; Alternate Processing Site:</p> <p>The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.</p> <p>References: NIST Special Publication 800-34.</p>	<p>CP-7 a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>a. 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: CP-7a. Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.</p>
<p>CP-8; CONTINGENCY PLANNING; Telecommunications Services:</p> <p>The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.</p> <p>References: NIST Special Publication 800-34; National Communications Directive 3-10; Web: TSP.NCS.GOV.</p>	<p>CP-8 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: CP-8. Requirement: The service provider defines a time period consistent with the business impact analysis.</p>

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

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

<p>IA-3 (1); IDENTIFICATION AND AUTHENTICATION; Device Identification And Authentication - Enhancement: Cryptographic Bidirectional Authentication</p> <p>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.</p> <p>References: None.</p>	<p>IA-3 (1) Not appropriate for DoD to define for all CSP's services.</p> <p>Source: DoD Broker Note the DoD RMF value is not valid for Cloud Computing. -----</p>
<p>IA-4; IDENTIFICATION AND AUTHENTICATION; Identifier Management:</p> <p>The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].</p> <p>References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.</p>	<p>IA-4 a. ISSM or ISSO d. 1 year for user identifiers (DoD is not going to specify value for device identifier). e. 35 days</p> <p>Source: DoD RMF TAG -----</p> <p>IA-4d. [at least two years] IA-4e. [ninety days for user identifiers] (See additional requirements and guidance.)</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: IA-4e. Requirement: The service provider defines time period of inactivity for device identifiers.</p>
<p>IA-4 (4); IDENTIFICATION AND AUTHENTICATION; Identifier Management - Enhancement: Identify User Status</p> <p>The organization manages individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].</p> <p>References: None.</p>	<p>IA-4 (4) contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil</p> <p>Source: DoD RMF TAG -----</p> <p>IA-4 (4). [contractors; foreign nationals]</p> <p>Source: FedRAMP v2 -----</p>

<p>IA-5; IDENTIFICATION AND AUTHENTICATION; Authenticator Management:</p> <p>The organization manages information system authenticators by:</p> <ul style="list-style-type: none">a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;b. Establishing initial authenticator content for authenticators defined by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;e. Changing default content of authenticators prior to information system installation;f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;g. Changing/refreshing authenticators <p>[Assignment: organization-defined time period by authenticator type];</p> <ul style="list-style-type: none">h. Protecting authenticator content from unauthorized disclosure and modification; andi. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; andj. Changing authenticators for group/role accounts when membership to those accounts changes. <p>References: OMB Memorandum 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov</p>	<p>IA-5 g. CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.</p> <p>Source: DoD RMF TAG -----</p> <p>IA-5g. [to include sixty days for passwords]</p> <p>Source: FedRAMP v2 -----</p>
<p>IA-5 (1); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Password-Based Authentication</p> <p>The information system, for password-based authentication:</p> <ul style="list-style-type: none">(a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];(b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];(c) Stores and transmits only encrypted representations of passwords;(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];(e) Prohibits password reuse for [Assignment: organization-defined number] generations; and(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password. <p>References: None.</p>	<p>IA-5 (1) As supported by the device:</p> <ul style="list-style-type: none">a. minimum of 15 Characters, 1 of each of the following character sets:<ul style="list-style-type: none">- Upper-case- Lower-case- Numerics- Special characters (e.g. ~ ! @ # \$ % ^ & * () _ + = - ' [] / ? > <);b. 50% of the minimum password length,d. Minimum 24 hours, Maximum 60 dayse. Minimum of 5 <p>Source: DoD RMF TAG -----</p> <p>IA-5 (1) (a). [case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters] IA-5 (1) (b). [at least one] IA-5 (1) (d). [one day minimum, sixty day maximum] IA-5 (1) (e). [twenty four]</p> <p>Source: FedRAMP v2 -----</p>

<p>IA-5 (3); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: In-Person Or Trusted Third-Party Registration</p> <p>The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: - in person; - by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>IA-5 (3) The DoD PKI CP defines the role and responsibilities of a DoD PKI Registration Authority (RA). The NSS PKI CP defines the role and responsibilities of an NSS PKI RA.</p> <p>The DoD PKI RA–LRA CPS defines the nomination process for DoD PKI RAs. The NSS PKI DoD RPS defines the nomination process for NSS PKI RAs for DoD.</p> <p>The DoD PKI CP defines DoD PKI subscribers and the authentication requirements for issuance of credentials to subscribers. The NSS PKI CP defines NSS PKI subscribers and the authentication requirements for issuance of credentials to subscribers.</p> <p>Source: DoD RMF TAG -----</p> <p>IA-5 (3). [All hardware/biometric (multifactor authenticators) [in person]]</p> <p>Source: FedRAMP v2 -----</p>
<p>IA-5 (4); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Automated Support For Password Strength Determination</p> <p>The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements].</p> <p>References: None.</p>	<p>IA-5 (4) complexity as identified in IA-5 (1) Part A</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: IA-4e Additional FedRAMP Requirements and Guidance: Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators</p>
<p>IA-5 (11); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Hardware Token-Based Authentication</p> <p>The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].</p> <p>References: None.</p>	<p>IA-5 (11) DoDI 8520.03</p> <p>Source: DoD RMF TAG -----</p>
<p>IA-5 (13); IDENTIFICATION AND AUTHENTICATION; Authenticator Management - Enhancement: Expiration Of Cached Authenticators</p> <p>The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].</p> <p>References: None.</p>	<p>IA-5 (13) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>IA-8 (3); IDENTIFICATION AND AUTHENTICATION; Identification And Authentication (Non-Organization Users) - Enhancement: Use Of FICAM-Approved Products</p> <p>The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.</p> <p>References: None.</p>	<p>IA-8 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>IR-1; INCIDENT RESPONSE; Incident Response Policy And Procedures:</p> <p>The organization:</p> <p>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;</p> <p>and</p> <p>b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency].</p> <p>References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.</p>	<p>IR-1</p> <p>a. all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>IR-1.b.1 [at least every 3 years] IR-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>IR-2; INCIDENT RESPONSE; Incident Response Training:</p> <p>The organization provides incident response training to information system users consistent with assigned roles and responsibilities:</p> <p>a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;</p> <p>b. When required by information system changes; and</p> <p>c. [Assignment: organization-defined frequency] thereafter.</p> <p>References: NIST Special Publications 800-16, 800-50.</p>	<p>IR-2</p> <p>a. 30 working days</p> <p>c. Annually</p> <p>Source: DoD RMF TAG -----</p> <p>IR-2b. [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>IR-3; INCIDENT RESPONSE; Incident Response Testing And Exercises RENAMED: Incident Response Testing:</p> <p>The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.</p> <p>References: NIST Special Publications 800-84, 800-115.</p>	<p>IR-3</p> <p>At least every six months for high availability and at least annually for low/med availability</p> <p>Tests as defined in the incident response plan</p> <p>Source: DoD RMF TAG -----</p> <p>IR-3. [at least annually]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: IR-3. Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Requirement: For JAB Authorization, the service provider provides test plans to the Authorizing Official (AO) annually.</p> <p>Requirement: Test plans are approved and accepted by the Authorizing Official prior to test commencing.</p>

<p>IR-4 (3); INCIDENT RESPONSE; Incident Handling - Enhancement: Continuity Of Operations</p> <p>The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions.</p> <p>References: None.</p>	<p>IR-4 (3) Classes of incidents defined in CJCSM 6510.01B Appendix A- Enclosure B</p> <p>Actions defined in CJCSM 6510.01B</p> <p>Source: DoD RMF TAG -----</p>
<p>IR-4 (7); INCIDENT RESPONSE; Incident Handling - Enhancement: Insider Threats - Intra-Organization Coordination</p> <p>The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization].</p> <p>References: None.</p>	<p>IR-4 (7) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>IR-4 (8); INCIDENT RESPONSE; Incident Handling - Enhancement: Correlation With External Organizations</p> <p>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.</p> <p>References: None.</p>	<p>IR-4 (8) The appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT)</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>IR-6; INCIDENT RESPONSE; Incident Reporting:</p> <p>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].</p> <p>References: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.</p>	<p>IR-6 a. the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance b. The appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT)</p> <p>Source: DoD RMF TAG -----</p> <p>IR-6a. [US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Requirement: Reports security incident information according to FedRAMP Incident Communications Procedure.</p>
<p>IR-6 (2); INCIDENT RESPONSE; Incident Reporting - Enhancement: Vulnerabilities Related To Incidents</p> <p>The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>IR-6 (2) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>IR-8; INCIDENT RESPONSE; Incident Response Plan:</p> <p>The organization:</p> <p>a. Develops an incident response plan that:</p> <ol style="list-style-type: none"> 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; <p>b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];</p> <p>c. Reviews the incident response plan [Assignment: organization-defined frequency];</p> <p>d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;</p> <p>e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];</p> <p>and</p> <p>f. Protects the incident response plan from unauthorized disclosure and modification.</p> <p>References: NIST Special Publication 800-61</p>	<p>IR-8</p> <ol style="list-style-type: none"> a. at a minimum, the ISSM and ISSO b. all stakeholders identified in the incident response plan c. at least annually (incorporating lessons learned from past incidents) e. all stakeholders identified in the incident response plan, not later than 30 days after the change is made <p>Source: DoD RMF TAG -----</p> <p>IR-8c. [at least annually]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: IR-8(b) Additional FedRAMP Requirements and Guidance: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. IR-8(e) Additional FedRAMP Requirements and Guidance: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.</p>
<p>IR-9; INCIDENT RESPONSE; Information Spillage Response:</p> <p>The organization responds to information spills by:</p> <ol style="list-style-type: none"> a. Identifying the specific information involved in the information system contamination; b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other [Assignment: organization-defined actions]. <p>References: None.</p>	<p>IR-9</p> <ol style="list-style-type: none"> b. at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center f. Not appropriate for DoD to define for all CSP's infrastructure or service offerings <p>Source: DoD RMF TAG -----</p>

<p>IR-9 (1); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Responsible Personnel</p> <p>The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.</p> <p>References: None.</p>	<p>IR-9 (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>IR-9 (2); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Training</p> <p>The organization provides information spillage response training [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>IR-9 (2) Annually</p> <p>Source: DoD RMF TAG -----</p>
<p>IR-9 (3); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Post-Spill Operations</p> <p>The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.</p> <p>References: None.</p>	<p>IR-9 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>IR-9 (4); INCIDENT RESPONSE; Information Spillage Response - Enhancement: Exposure To Unauthorized Personnel</p> <p>The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.</p> <p>References: None.</p>	<p>IR-9 (4) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>MA-1; MAINTENANCE; System Maintenance Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; <p>and</p> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency]. <p>References: NIST Special Publications 800-12, 800-100.</p>	<p>MA-1</p> <ol style="list-style-type: none"> a. all stakeholders identified in the maintenance policy b. (1) every 5 years b. (2) annually <p>Source: DoD RMF TAG -----</p> <p>MA-1.b.1 [at least every 3 years] MA-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>MA-2; MAINTENANCE; Controlled Maintenance:</p> <p>The organization:</p> <p>a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;</p> <p>b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;</p> <p>c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;</p> <p>d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;</p> <p>e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and</p> <p>f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.</p> <p>References: None.</p>	<p>MA-2</p> <p>c. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>f. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>MA-3 (3); MAINTENANCE; Maintenance Tools - Enhancement: Prevent Unauthorized Removal</p> <p>The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:</p> <p>(a) Verifying that there is no organizational information contained on the equipment;</p> <p>(b) Sanitizing or destroying the equipment;</p> <p>(c) Retaining the equipment within the facility; or</p> <p>(d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.</p> <p>References: None.</p>	<p>MA-3 (3)</p> <p>d. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>MA-3 (3) (d). [the information owner explicitly authorizing removal of the equipment from the facility]</p> <p>Source: FedRAMP v2 -----</p>
<p>MA-6; MAINTENANCE; Timely Maintenance:</p> <p>The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.</p> <p>References: None.</p>	<p>MA-6</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability)</p> <p>Source: DoD RMF TAG -----</p>

<p>MP-1; MEDIA PROTECTION; Media Protection Policy And Procedures:</p> <p>The organization:</p> <p>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;</p> <p>and</p> <p>b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency].</p> <p>References: NIST Special Publications 800-12, 800-100.</p>	<p>MP-1 a. all users</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>MP-1.b.1 [at least every 3 years] MP-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>MP-2; MEDIA PROTECTION; Media Access:</p> <p>The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined personnel or roles].</p> <p>References: FIPS Publication 199; NIST Special Publication 800-111</p>	<p>MP-2 All types of digital and/or non-digital media containing information not cleared for public release</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings, but types of media must be identified IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001</p> <p>Source: DoD RMF TAG -----</p>
<p>MP-3; MEDIA PROTECTION; Media Marking:</p> <p>The organization:</p> <p>a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and</p> <p>b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].</p> <p>References: FIPS Publication 199.</p>	<p>MP-3 b. nothing unless otherwise exempted by DoDI 5200.01 and DoDM 5200.01 Vol 1-4</p> <p>b. all areas unless otherwise exempted by DoDI 5200.01 and DoDM 5200.01 Vol 1-4</p> <p>Source: DoD RMF TAG -----</p> <p>MP-3b. [no removable media types]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: MP-3b. Guidance: Second parameter not-applicable</p>

<p>MP-4; MEDIA PROTECTION; Media Storage:</p> <p>The organization:</p> <p>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.</p> <p>References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-11</p>	<p>MP-4</p> <p>a (1). all digital and non-digital media containing sensitive, controlled, and/or classified information.</p> <p>a (2). areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media.</p> <p>Source: DoD RMF TAG -----</p> <p>MP-4a. [all types of digital and non-digital media with sensitive information] within [FedRAMP Assignment: see additional FedRAMP requirements and guidance];</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: MP-4a Additional FedRAMP Requirements and Guidance: Requirement: The service provider defines controlled areas within facilities where the information and information system reside.</p>
<p>MP-5; MEDIA PROTECTION; Media Transport:</p> <p>The organization:</p> <p>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.</p> <p>References: FIPS Publication 199; NIST Special Publication 800-60.</p>	<p>MP-5</p> <p>a. all digital and non-digital media containing sensitive, controlled, and/or classified information.</p> <p>a. DoDI 5200.1R and other organizationally defined security safeguards.</p> <p>Source: DoD RMF TAG -----</p> <p>MP-5a. [all media with sensitive information] [prior to leaving secure/controlled environment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container]</p> <p>Source: FedRAMP v2 -----</p>
<p>MP-6; MEDIA PROTECTION; Media Sanitization:</p> <p>The organization:</p> <p>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.</p> <p>References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.</p>	<p>MP-6</p> <p>a. all media</p> <p>a. techniques and procedures IAW NIST SP 800-88</p> <p>Source: DoD RMF TAG -----</p> <p>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.</p> <p>Source: FedRAMP v2 -----</p>

<p>MP-6 (2); MEDIA PROTECTION; Media Sanitization - Enhancement: Equipment Testing</p> <p>The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved.</p> <p>References: None.</p>	<p>MP-6 (2) every 180 days.</p> <p>Source: DoD RMF TAG -----</p> <p>[At least annually]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Guidance: Equipment and procedures may be tested or validated for effectiveness</p>
<p>MP-7; MEDIA PROTECTION; Media Use:</p> <p>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].</p> <p>References: FIPS Publication 199; NIST Special Publication 800-111.</p>	<p>MP-7 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>PE-1; PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical And Environmental Protection Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; <p>and</p> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency]. <p>References: NIST Special Publications 800-12, 800-100.</p>	<p>PE-1 a. all personnel</p> <p>b. (1) annually b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>PE-1.b.1 [at least every 3 years] PE-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>PE-2; PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical Access Authorizations:</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; <p>and</p> <ul style="list-style-type: none"> d. Removes individuals from the facility access list when access is no longer required. <p>References: None.</p>	<p>PE-2 c. every 90 days</p> <p>Source: DoD RMF TAG -----</p> <p>PE-2c. [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>PE-3; PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical Access Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] <p>by;</p> <ul style="list-style-type: none"> 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): - [Assignment: organization-defined physical access control systems/devices]; - guards]; <ul style="list-style-type: none"> b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. <p>References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov</p>	<p>PE-3</p> <ul style="list-style-type: none"> a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings a. (2) Not appropriate for DoD to define for all CSP's infrastructure or service offerings b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings c. Not appropriate for DoD to define for all CSP's infrastructure or service offerings d. Not appropriate for DoD to define for all CSP's infrastructure or service offerings f. minimally keys or any other physical token used to gain access f. annually g. as required by security relevant events <p>Source: DoD RMF TAG -----</p> <p>PE-3a.2 [CSP defined physical access control systems/devices AND guards] PE-3d. [in all circumstances within restricted access area where the information system resides] PE-3f. [at least annually]</p> <p>PE-3g. [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>PE-3 (1); PHYSICAL AND ENVIRONMENTAL PROTECTION; Physical Access Control - Enhancement: Information System Access</p> <p>The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the information system].</p> <p>References: None.</p>	<p>PE-3 (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>PE-4; PHYSICAL AND ENVIRONMENTAL PROTECTION; Access Control For Transmission Medium:</p> <p>The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].</p> <p>References: NSTISSI No. 7003.</p>	<p>PE-4 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>PE-6; PHYSICAL AND ENVIRONMENTAL PROTECTION; Monitoring Physical Access:</p> <p>The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.</p> <p>References: None.</p>	<p>PE-6 b. every 30 days</p> <p>b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>PE-6b.[at least monthly]</p> <p>Source: FedRAMP v2 -----</p>
<p>PE-8; PHYSICAL AND ENVIRONMENTAL PROTECTION; Access Records RENAMED: Visitor Access Records:</p> <p>The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>PE-8 a. at least one year b. every 30 days</p> <p>Source: DoD RMF TAG -----</p> <p>PE-8a [for a minimum of one year] PE-8b. [at least monthly]</p> <p>Source: FedRAMP v2 -----</p>

<p>PE-10; PHYSICAL AND ENVIRONMENTAL PROTECTION; Emergency Shutoff:</p> <p>The organization:</p> <p>a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;</p> <p>b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and</p> <p>c. Protects emergency power shutoff capability from unauthorized activation.</p> <p>References: None.</p>	<p>PE-10</p> <p>b. or near more than one egress point of the IT area and it is labeled and protected by a cover to prevent accidental shut-off</p> <p>Source: DoD RMF TAG -----</p>
<p>PE-13 (2); PHYSICAL AND ENVIRONMENTAL PROTECTION; Fire Protection - Enhancement: Suppression Devices / Systems</p> <p>The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].</p> <p>References: None.</p>	<p>PE-13 (2)</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>PE-14; PHYSICAL AND ENVIRONMENTAL PROTECTION; Temperature And Humidity Controls:</p> <p>The organization:</p> <p>a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and</p> <p>b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>PE-14</p> <p>a. For commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; For other systems, levels within manufacturer specifications</p> <p>b. Continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required</p> <p>Source: DoD RMF TAG -----</p> <p>PE-14a. [consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments]</p> <p>PE-14b. [continuously]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: PE-14a. Requirements: The service provider measures temperature at server inlets and humidity levels by dew point.</p>
<p>PE-16; PHYSICAL AND ENVIRONMENTAL PROTECTION; Delivery And Removal:</p> <p>The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.</p> <p>References: None.</p>	<p>PE-16</p> <p>All system components</p> <p>Source: DoD RMF TAG -----</p> <p>PE-16. [all information system components]</p> <p>Source: FedRAMP v2 -----</p>

<p>PE-17; PHYSICAL AND ENVIRONMENTAL PROTECTION; Alternate Work Site:</p> <p>The organization:</p> <p>a. Employs [Assignment: organization-defined security controls] at alternate work sites;</p> <p>b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and</p> <p>c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.</p> <p>References: NIST Special Publication 800-46.</p>	<p>PE-17</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings but must include all applicable building and safety codes for the information system's environment</p> <p>Source: DoD RMF TAG -----</p>
<p>PL-1; PLANNING; Security Planning Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; <p>and</p> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Security planning policy [Assignment: organization-defined frequency]; <p>and</p> <ol style="list-style-type: none"> 2. Security planning procedures [Assignment: organization-defined frequency]. <p>References: NIST Special Publications 800-12, 800-18, 800-100</p>	<p>PL-1</p> <p>a. all personnel</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>PL-1.b.1 [at least every 3 years] PL-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>PL-2; PLANNING; System Security Plan:</p> <p>The organization:</p> <p>a. Develops a security plan for the information system that:</p> <ol style="list-style-type: none"> 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; <p>b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];</p> <p>c. Reviews the security plan for the information system [Assignment: organization-defined frequency];</p> <p>d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and</p> <p>e. Protects the security plan from unauthorized disclosure and modification.</p> <p>References: NIST Special Publication 800-18.</p>	<p>PL-2</p> <p>b. at a minimum, the ISSO, ISSM and SCA</p> <p>c. annually</p> <p>Source: DoD RMF TAG -----</p> <p>PL-2c. [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>PL-2 (3); PLANNING; System Security Plan - Enhancement: Plan / Coordinate With Other Organizational Entities</p> <p>The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.</p> <p>References: None.</p>	<p>PL-2 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>PL-4; PLANNING; Rules Of Behavior:</p> <p>The organization:</p> <ol style="list-style-type: none"> Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. <p>References: NIST Publication 800-18.</p>	<p>PL-4 c. annually</p> <p>Source: DoD RMF TAG -----</p> <p>PL-4c. [At least every 3 years]</p> <p>Source: FedRAMP v2 -----</p>
<p>PL-8; PLANNING; Information Security Architecture:</p> <p>The organization:</p> <ol style="list-style-type: none"> Develops an information security architecture for the information system that: <ol style="list-style-type: none"> Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; Describes how the information security architecture is integrated into and supports the enterprise architecture; and Describes any information security assumptions about, and dependencies on, external services; Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. <p>References: None.</p>	<p>PL-8 b. annually</p> <p>Source: DoD RMF TAG -----</p> <p>PL-8b. [At least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>PL-8 (1); PLANNING; Information Security Architecture - Enhancement: Defense-In-Depth</p> <p>The organization designs its security architecture using a defense-in-depth approach that:</p> <p>(a) Allocates [Assignment: organization-defined security safeguards]</p> <p>to [Assignment: organization-defined locations and architectural layers];</p> <p>and</p> <p>(b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.</p> <p>References: None.</p>	<p>PL-8 (1)</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>PS-1; PERSONNEL SECURITY; Personnel Security Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency]. <p>References: None.</p>	<p>PS-1</p> <p>a. all personnel</p> <p>b. (1) every 5 years b (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>PS-1.b.1 [at least every 3 years] PS-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>PS-2; PERSONNEL SECURITY; Position Categorization RENAMED: Position Risk Designation:</p> <p>The organization:</p> <p>a. Assigns a risk designation to all organizational positions;</p> <p>b. Establishes screening criteria for individuals filling those positions; and</p> <p>c. Reviews and updates position risk designations [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>PS-2</p> <p>c. Annually</p> <p>Source: DoD RMF TAG -----</p> <p>PS-2c. [at least every three years]</p> <p>Source: FedRAMP v2 -----</p>
<p>PS-3; PERSONNEL SECURITY; Personnel Screening:</p> <p>The organization:</p> <p>a. Screens individuals prior to authorizing access to the information system; and</p> <p>b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].</p> <p>References: None.</p>	<p>PS-3</p> <p>b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>PS-3b. [for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance.</p> <p>For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions]</p> <p>Source: FedRAMP v2 -----</p>

<p>PS-3 (3); PERSONNEL SECURITY; Personnel Screening - Enhancement: Information With Special Protection Measures</p> <p>The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:</p> <p>(a) Have valid access authorizations that are demonstrated by assigned official government duties; and</p> <p>(b) Satisfy [Assignment: organization-defined additional personnel screening criteria].</p> <p>References: None.</p>	<p>PS-3 (3) b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>PS-3 (3)(b). [personnel screening criteria – as required by specific information]</p> <p>Source: FedRAMP v2 -----</p>
<p>PS-4; PERSONNEL SECURITY; Personnel Termination:</p> <p>The organization, upon termination of individual employment:</p> <p>a. Disables information system access within [Assignment: organization-defined time period];</p> <p>b. Terminates/revokes any authenticators/credentials associated with the individual;</p> <p>c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];</p> <p>d. Retrieves all security-related organizational information system-related property;</p> <p>e. Retains access to organizational information and information systems formerly controlled by terminated individual; and</p> <p>f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].</p> <p>References: NIST Special Publication 800-35.</p>	<p>PS-4 a. immediately</p> <p>c. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>f. at a minimum, the ISSO and personnel responsible for revoking credentials</p> <p>f. immediately or within 24 hours</p> <p>Source: DoD RMF TAG -----</p> <p>PS-4.a. [same day]</p> <p>Source: FedRAMP v2 -----</p>
<p>PS-5; PERSONNEL SECURITY; Personnel Transfer:</p> <p>The organization:</p> <p>a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;</p> <p>b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];</p> <p>c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and</p> <p>d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].</p> <p>References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.</p>	<p>PS-5 b. actions to ensure all system accesses no longer required are removed</p> <p>b. immediately</p> <p>d. at a minimum, the ISSO and personnel responsible for transferring credentials</p> <p>d. 24 hours</p> <p>Source: DoD RMF TAG -----</p> <p>PS-5. [within five days of the formal transfer action (DoD 24 hours)]</p> <p>Source: FedRAMP v2 -----</p>

<p>PS-6; PERSONNEL SECURITY; Access Agreements:</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: <ul style="list-style-type: none"> 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency]. <p>References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web: idmanagement.gov.</p>	<p>PS-6 b. annually</p> <p>c (2) when there is a change to the user's level of access</p> <p>Source: DoD RMF TAG -----</p> <p>PS-6b. [at least annually] PS-6c.2. [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>PS-7; PERSONNEL SECURITY; Third-Party Personnel Security:</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and e. Monitors provider compliance. <p>References: None.</p>	<p>PS-7 d. at a minimum, the ISSO and personnel responsible for transferring credentials</p> <p>d. immediately</p> <p>Source: DoD RMF TAG -----</p> <p>PS-7d. organization-defined time period – same day</p> <p>Source: FedRAMP v2 -----</p>
<p>PS-8; PERSONNEL SECURITY; Personnel Sanctions:</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. <p>References: None.</p>	<p>PS-8 b. at a minimum, the ISSO</p> <p>b. immediately</p> <p>Source: DoD RMF TAG -----</p>

<p>RA-1; RISK ASSESSMENT; Risk Assessment Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls;</p> <p>and</p> <p>b. Reviews and updates the current:</p> <p>1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>RA-1</p> <p>a. at a minimum, the ISSM and ISSO</p> <p>b. (1) every five years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>RA-1.b.1 [at least every 3 years] RA-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>RA-3; RISK ASSESSMENT; Risk Assessment:</p> <p>The organization:</p> <p>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;</p> <p>b. Documents risk assessment results in [Selection: - security plan; - risk assessment report; - [Assignment: organization-defined document]];</p> <p>c. Reviews risk assessment results [Assignment: organization-defined frequency];</p> <p>d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and</p> <p>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.</p> <p>References: None.</p>	<p>RA-3</p> <p>b. a risk assessment report c. upon re-accreditation d. ISSM, ISSO, AO, and PM e. upon re-accreditation</p> <p>Source: DoD RMF TAG -----</p> <p>RA-3b. [security assessment report]</p> <p>RA-3c. [at least every three years or when a significant change occurs]</p> <p>RA-3e. [at least every three years or when a significant change occurs]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.</p> <p>RA-3d. Requirement: to include the Authorizing Official; for JAB authorizations to include FedRAMP</p>

<p>RA-5; RISK ASSESSMENT; Vulnerability Scanning:</p> <p>The organization:</p> <p>a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;</p> <p>b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:</p> <ol style="list-style-type: none"> 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; <p>c. Analyzes vulnerability scan reports and results from security control assessments;</p> <p>d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and</p> <p>e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).</p> <p>References: None.</p>	<p>RA-5</p> <p>a. every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs)</p> <p>d. IAW an authoritative source (e.g. IAVM, CTOs, DTMs)</p> <p>e. at a minimum, the ISSM and ISSO</p> <p>Source: DoD RMF TAG -----</p> <p>RA-5a. [monthly operating system/infrastructure; monthly web applications and databases]</p> <p>RA-5d. [high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate-risk vulnerabilities mitigated within ninety days from date of discovery]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: RA-5a. Requirement: an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually. RA-5e. Requirement: to include the Risk Executive; for JAB authorizations to include FedRAMP</p>
<p>RA-5 (2); RISK ASSESSMENT; Vulnerability Scanning - Enhancement: Update By Frequency / Prior To New Scan / When Identified</p> <p>The organization updates the information system vulnerabilities scanned [Selection (one or more): - [Assignment: organization-defined frequency]; - prior to a new scan; - when new vulnerabilities are identified and reported].</p> <p>References: None.</p>	<p>RA-5 (2) prior to running scans</p> <p>Source: DoD RMF TAG -----</p> <p>RA-5 (2). [prior to a new scan]</p> <p>Source: FedRAMP v2 -----</p>
<p>RA-5 (5); RISK ASSESSMENT; Vulnerability Scanning - Enhancement: Privileged Access</p> <p>The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities].</p> <p>References: NIST Special Publication 800-65.</p>	<p>RA-5 (5) all information systems and infrastructure components</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>RA-5 (5). [operating systems / web applications / databases] [all scans]</p> <p>Source: FedRAMP v2 -----</p>

<p>SA-1; SYSTEM AND SERVICES ACQUISITION; System And Services Acquisition Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls;</p> <p>and</p> <p>b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency].</p> <p>References: None.</p>	<p>SA-1</p> <p>a. all personnel</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>SA-1.b.1 [at least every 3 years] SA-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>SA-3; SYSTEM AND SERVICES ACQUISITION; Life Cycle Support RENAMED: System Development Life Cycle:</p> <p>The organization:</p> <p>a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;</p> <p>b. Defines and documents information security roles and responsibilities throughout the system development life cycle;</p> <p>c. Identifies individuals having information security roles and responsibilities; and</p> <p>d. Integrates the organizational information security risk management process into system development life cycle activities.</p> <p>References: None.</p>	<p>SA-3</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SA-4 (2); SYSTEM AND SERVICES ACQUISITION; Acquisitions RENAMED: Acquisition Process - Enhancement: Design / Implementation Information For Security Controls</p> <p>The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes:</p> <p>[Selection (one or more): - security-relevant external system interfaces; - high-level design; - low-level design; - source code or hardware schematics; - [Assignment: organization-defined design/implementation information]]</p> <p>at [Assignment: organization-defined level of detail].</p> <p>References: None.</p>	<p>SA-4 (2)</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>[to include security-relevant external system interfaces and high-level design]</p> <p>Source: FedRAMP v2 -----</p>

<p>SA-4 (8); SYSTEM AND SERVICES ACQUISITION; Acquisition Process - Enhancement: Continuous Monitoring Plan</p> <p>The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [Assignment: organization-defined level of detail].</p> <p>References: None.</p>	<p>SA-4 (8) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>SA-4 (8). [at least the minimum requirement as defined in control CA-7]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: SA-4 (8) Guidance: CSP must use the same security standards regardless of where the system component or information system service is aquired.</p>
<p>SA-5; SYSTEM AND SERVICES ACQUISITION; Information System Documentation:</p> <p>The organization:</p> <p>a. Obtains administrator documentation for the information system, system component, or information system service that describes:</p> <ol style="list-style-type: none">1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security functions/mechanisms; and3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; <p>b. Obtains user documentation for the information system, system component, or information system service that describes:</p> <ol style="list-style-type: none">1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and3. User responsibilities in maintaining the security of the system, component, or service; <p>c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;</p> <p>d. Protects documentation as required, in accordance with the risk management strategy; and</p> <p>e. Distributes documentation to [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>SA-5 c. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>e. at a minimum, the ISSO, ISSM, and SCA</p> <p>Source: DoD RMF TAG -----</p>

<p>SA-9; SYSTEM AND SERVICES ACQUISITION; External Information System Services:</p> <p>The organization:</p> <p>a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;</p> <p>b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and</p> <p>c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.</p> <p>References: None.</p>	<p>SA-9</p> <p>a. security controls defined by CNSSI 1253</p> <p>c. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>SA-9a. [FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system] SA-9c. [Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored]</p> <p>Source: FedRAMP v2 -----</p>
<p>SA-9 (1); SYSTEM AND SERVICES ACQUISITION; External Information System Services - Enhancement: Risk Assessments / Organizational Approvals</p> <p>The organization:</p> <p>(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and</p> <p>(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].</p> <p>References: None.</p>	<p>SA-9 (1)</p> <p>b. the DoD Component CIO or their delegate(s)</p> <p>Source: DoD RMF TAG -----</p> <p>SA-9 (1) see Additional Requirement and Guidance</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: SA-9 (1). Requirement: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. For JAB authorizations, future planned outsourced services are approved and accepted by the JAB.</p>
<p>SA-9 (2); SYSTEM AND SERVICES ACQUISITION; External Information Systems - Enhancement: Identification Of Functions / Ports / Protocols / Services</p> <p>The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.</p> <p>References: None.</p>	<p>SA-9 (2)</p> <p>All external information system services</p> <p>Source: DoD RMF TAG -----</p> <p>SA-9 (2). [All external systems where Federal information is processed, transmitted or stored]</p> <p>Source: FedRAMP v2 -----</p>

<p>SA-9 (4); SYSTEM AND SERVICES ACQUISITION; External Information Systems - Enhancement: Consistent Interests Of Consumers And Providers</p> <p>The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests.</p> <p>References: None.</p>	<p>SA-9 (4) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>All external service providers from whom services are solicited.</p> <p>Source: DoD RMF TAG -----</p> <p>SA-9 (4). [All external systems where Federal information is processed, transmitted or stored]</p> <p>Source: FedRAMP v2 -----</p>
<p>SA-9 (5); SYSTEM AND SERVICES ACQUISITION; External Information Systems - Enhancement: Processing Storage And Service Location</p> <p>The organization restricts the location of [Selection (one or more): - information processing; - information/data; - information system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].</p> <p>References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org.</p>	<p>SA-9 (5) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p> <p>SA-9 (5). [information processing, transmission, information data, AND information services]</p> <p>Source: FedRAMP v2 -----</p>
<p>SA-10; SYSTEM AND SERVICES ACQUISITION; Developer Configuration Management:</p> <p>The organization requires the developer of the information system, system component, or information system service to:</p> <p>a. Perform configuration management during system, component, or service [Selection (one or more): - design; - development; - implementation; - operation];</p> <p>b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];</p> <p>c. Implement only organization-approved changes to the system, component, or service;</p> <p>d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and</p> <p>e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].</p> <p>References: None.</p>	<p>SA-10 b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>e. at a minimum, the ISSO and ISSM</p> <p>Source: DoD RMF TAG -----</p> <p>SA-10a. [development, implementation, AND operation]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: SA-10e. Requirement: for JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.</p>

<p>SA-11; SYSTEM AND SERVICES ACQUISITION; Developer Security Testing RENAMED: Developer Security Testing And Evaluation:</p> <p>The organization requires the developer of the information system, system component, or information system service to:</p> <ol style="list-style-type: none">Create and implement a security assessment plan;Perform [Selection (one or more):<ul style="list-style-type: none">- unit;- integration;- system;- regression] <p>testing/evaluation at [Assignment: organization-defined depth and coverage];</p> <ol style="list-style-type: none">Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;Implement a verifiable flaw remediation process; andCorrect flaws identified during security testing/evaluation. <p>References: None.</p>	<p>SA-11 b. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SA-12; SYSTEM AND SERVICES ACQUISITION; Supply Chain Protection:</p> <p>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.</p> <p>References: None.</p>	<p>SA-12 measures of protection IAW DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)"</p> <p>Source: DoD RMF TAG -----</p>
<p>SA-19; SYSTEM AND SERVICES ACQUISITION; Component Authenticity:</p> <p>The organization:</p> <ol style="list-style-type: none">Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; andReports counterfeit information system components to [Selection (one or more):<ul style="list-style-type: none">- source of counterfeit component;- [Assignment: organization-defined external reporting organizations];- [Assignment: organization-defined personnel or roles]]. <p>References: None.</p>	<p>SA-19 b. at a minimum, USCYBERCOM</p> <p>b. at a minimum, the ISSO, ISSM, and PM</p> <p>Source: DoD RMF TAG -----</p>

<p>SC-1; SYSTEM AND COMMUNICATIONS PROTECTION; System And Communications Protection Policy And Procedures:</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency]. <p>References: None.</p>	<p>SC-1</p> <p>a. at a minimum, the ISSM/ISSO</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>SC-1.b.1 [at least every 3 years] SC-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>
<p>SC-5; SYSTEM AND COMMUNICATIONS PROTECTION; Denial Of Service Protection:</p> <p>The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].</p> <p>References: None.</p>	<p>SC-5</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-6; SYSTEM AND COMMUNICATIONS PROTECTION; Resource Priority RENAMED: Resource Availability:</p> <p>The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); - priority; - quota; - [Assignment: organization-defined security safeguards]].</p> <p>References: None.</p>	<p>SC-6</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-7 (4); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: External Telecommunications Services</p> <p>The organization:</p> <ol style="list-style-type: none"> (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. <p>References: None.</p>	<p>SC-7 (4)</p> <p>e. every 180 days</p> <p>Source: DoD RMF TAG -----</p> <p>SC-7 (4). [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>SC-7 (8); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Route Traffic To Authenticated Proxy Servers</p> <p>The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.</p> <p>References: None.</p>	<p>SC-7 (8) protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP)</p> <p>any network external to the authorization boundary</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-7 (11); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Restrict Incoming Communications Traffic</p> <p>The information system only allows incoming communications from [Assignment: organization-defined authorized sources] routed to [Assignment: organization-defined authorized destinations].</p> <p>References: None.</p>	<p>SC-7 (11) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-7 (12); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Host-Based Protection</p> <p>The organization implements [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined information system components].</p> <p>References: None.</p>	<p>SC-7 (12) McAfee Host Intrusion Prevention (HIPS)</p> <p>All information system components.</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-7 (13); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Isolation Of Security Tools / Mechanisms / Support Components</p> <p>The organization isolates [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.</p> <p>References: None.</p>	<p>SC-7 (13) key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc.</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: SC-7 (13). Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.</p>
<p>SC-7 (14); SYSTEM AND COMMUNICATIONS PROTECTION; Boundary Protection - Enhancement: Protects Against Unauthorized Physical Connections</p> <p>The organization protects against unauthorized physical connections at [Assignment: organization-defined managed interfaces].</p> <p>References: None.</p>	<p>SC-7 (14) internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.</p> <p>Source: DoD RMF TAG -----</p>

<p>SC-8 (1); SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity - Enhancement: Cryptographic Or Alternate Physical Protection</p> <p>The information system implements cryptographic mechanisms to [Selection (one or more): - prevent unauthorized disclosure of information; - detect changes to information]</p> <p>during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].</p> <p>References: None.</p>	<p>SC-8 (1) Protected Distribution System (PDS)</p> <p>Source: DoD RMF TAG -----</p> <p>SC-8 (1). [prevent unauthorized disclosure of information AND detect changes to information] [a hardened or alarmed carrier Protective Distribution System (PDS)]</p> <p>Source: FedRAMP v2 -----</p>
<p>SC-8 (2); SYSTEM AND COMMUNICATIONS PROTECTION; Transmission Integrity RENAMED: Transmission Confidentiality And Integrity - Enhancement: Pre / Post Transmission Handling</p> <p>The information system maintains the [Selection (one or more): - confidentiality; - integrity]</p> <p>of information during preparation for transmission and during reception.</p> <p>References: None.</p>	<p>missing????</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-10; SYSTEM AND COMMUNICATIONS PROTECTION; Network Disconnect:</p> <p>The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.</p> <p>References: None.</p>	<p>SC-10 10 minutes in band management and 15 minutes for user sessions</p> <p>Source: DoD RMF TAG -----</p> <p>SC-10. [no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions]</p> <p>Source: FedRAMP v2 -----</p>
<p>SC-12; SYSTEM AND COMMUNICATIONS PROTECTION; Cryptographic Key Establishment And Management:</p> <p>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].</p> <p>References: None.</p>	<p>SC-12 DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems"</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: SC-12 Guidance: Federally approved cryptography</p>
<p>SC-12 (2); SYSTEM AND COMMUNICATIONS PROTECTION; Cryptographic Key Establishment And Management - Enhancement: Symmetric Keys</p> <p>The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: - NIST FIPS-compliant; - NSA-approved]</p> <p>key management technology and processes.</p> <p>References: None.</p>	<p>SC-12 (2) NIST Approved for Unclassified systems NSA Approved for Classified systems</p> <p>Source: DoD RMF TAG -----</p> <p>SC-12 (2). [NIST FIPS-compliant]</p> <p>Source: FedRAMP v2 -----</p>

<p>SC-13; SYSTEM AND COMMUNICATIONS PROTECTION; Use Of Cryptography RENAMED: Cryptographic Protection:</p> <p>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.</p> <p>References: None.</p>	<p>SC-13 Protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography</p> <p>Source: DoD RMF TAG -----</p> <p>[FIPS-validated or NSA-approved cryptography]</p> <p>Source: FedRAMP v2 -----</p>
<p>SC-15; SYSTEM AND COMMUNICATIONS PROTECTION; Collaborative Computing Devices:</p> <p>The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.</p> <p>References: NIST Special Publication 800-28; DOD Instruction 8552.01</p>	<p>SC-15 Dedicated VTC suites located in approved VTC locations that are centrally managed</p> <p>Source: DoD RMF TAG -----</p> <p>SC-15a. [no exceptions]</p> <p>Source: FedRAMP v2 -----</p>
<p>SC-17; SYSTEM AND COMMUNICATIONS PROTECTION; Public Key Infrastructure Certificates:</p> <p>The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.</p> <p>References: OMB Memorandum 08-23; NIST Special Publication 800-81</p>	<p>SC-17 DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling.</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-18 (4); SYSTEM AND COMMUNICATIONS PROTECTION; Mobile Code - Enhancement: Prevent Automatic Execution</p> <p>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.</p> <p>References: NIST Special Publication 800-81</p>	<p>SC-18 (4) DoDI 8552.01 "Use of Mobile Code Technologies in DoD Information Systems"</p> <p>the user be prompted</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-23 (3); SYSTEM AND COMMUNICATIONS PROTECTION; Session Authenticity - Enhancement: Unique Session Identifiers With Randomization</p> <p>The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session identifiers that are system-generated.</p> <p>References: NIST Special Publications 800-56, 800-57, 800-111</p>	<p>SC-23 (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>SC-23 (5); SYSTEM AND COMMUNICATIONS PROTECTION; Session Authenticity - Enhancement: Allowed Certificate Authorities</p> <p>The information system only allows the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.</p> <p>References: None.</p>	<p>SC-23 (5) DoD PKI established certificate authorities.</p> <p>Source: DoD RMF TAG -----</p>
<p>SC-28; SYSTEM AND COMMUNICATIONS PROTECTION; Protection Of Information At Rest:</p> <p>The information system protects the [Selection (one or more): - confidentiality; - integrity] of [Assignment: organization-defined information at rest].</p> <p>References: None.</p>	<p>SC-28 Not appropriate for DoD to define for all CSP's infrastructure or service offerings. At a minimum, must include PII and classified information.</p> <p>Source: DoD RMF TAG -----</p> <p>SC-28. [confidentiality AND integrity]</p> <p>Source: FedRAMP v2 -----</p> <p>FedRAMP Additional Requirements and Guidance: SC-28. Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.</p>
<p>SC-28 (1); SYSTEM AND COMMUNICATIONS PROTECTION; Protection Of Information At Rest - Enhancement: Cryptographic Protection</p> <p>The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [Assignment: organization-defined information system components].</p> <p>References: None.</p>	<p>SC-28 (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings. At a minimum, PII and classified information.</p> <p>any information system components storing data defined in SC-28 (1), 2473</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-1; SYSTEM AND INFORMATION INTEGRITY; System And Information Integrity Policy And Procedures:</p> <p>The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency].</p> <p>References: NIST Special Publication 800-83.</p>	<p>SI-1 a. all appointed information assurance personnel</p> <p>b. (1) every 5 years b. (2) annually</p> <p>Source: DoD RMF TAG -----</p> <p>SI-1.b.1 [at least every 3 years] SI-1.b.2 [at least annually]</p> <p>Source: FedRAMP v2 -----</p>

<p>SI-2; SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation:</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. <p>References: None.</p>	<p>SI-2</p> <p>c. within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs)</p> <p>Source: DoD RMF TAG -----</p> <p>SI-2c. [Within 30 days of release of updates]</p> <p>Source: FedRAMP v2 -----</p>
<p>SI-2 (2); SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation - Enhancement: Automated Flaw Remediation Status</p> <p>The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.</p> <p>References: None.</p>	<p>SI-2 (2)</p> <p>Continuously with HBSS 30 days for any additional internal network scans not covered by HBSS Annually for external scans by (Computer Network Defense Service Provider) CNDSP</p> <p>Source: DoD RMF TAG -----</p> <p>SI-2 (2). [at least monthly]</p> <p>Source: FedRAMP v2 -----</p>
<p>SI-2 (3); SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation - Enhancement: Time To Remediate Flaws / Benchmarks For Corrective Actions</p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Measures the time between flaw identification and flaw remediation; and (b) Establishes [Assignment: organization-defined benchmarks] for taking corrective actions. <p>References: None.</p>	<p>SI-2 (3)</p> <p>b. within the period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs)</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-2 (6); SYSTEM AND INFORMATION INTEGRITY; Flaw Remediation - Enhancement: Removal Of Previous Versions Of Software / Firmware</p> <p>The organization removes [Assignment: organization-defined software and firmware components] after updated versions have been installed.</p> <p>References: None.</p>	<p>SI-2 (6)</p> <p>All upgraded/replaced software and firmware components that are no longer required for operation</p> <p>Source: DoD RMF TAG -----</p>

<p>SI-3; SYSTEM AND INFORMATION INTEGRITY; Malicious Code Protection:</p> <p>The organization:</p> <ul style="list-style-type: none">a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;c. Configures malicious code protection mechanisms to:<ul style="list-style-type: none">1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more);<ul style="list-style-type: none">- endpoint;- network entry/exit points <p>as the files are downloaded, opened, or executed in accordance with organizational security policy; and</p> <ul style="list-style-type: none">2. [Selection (one or more):<ul style="list-style-type: none">- block malicious code;- quarantine malicious code;- send alert to administrator;- [Assignment: organization-defined action] <p>in response to malicious code detection; and</p> d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. <p>References: None.</p>	<p>SI-3 c (1). every 7 days c (2). Block and quarantine malicious code and then send an alert to the administrator immediately in near real-time</p> <p>Source: DoD RMF TAG -----</p> <p>SI-3.c.1 [at least weekly] [to include endpoints] SI-3.c.2 [to include alerting administrator or defined security personnel]</p> <p>Source: FedRAMP v2 -----</p>
<p>SI-3 (10); SYSTEM AND INFORMATION INTEGRITY; Malicious Code Protection - Enhancement: Malicious Code Analysis</p> <p>The organization:</p> <ul style="list-style-type: none">(a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of malicious code; and(b) Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes. <p>References: None.</p>	<p>SI-3 (10) a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>

<p>SI-4; SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring:</p> <p>The organization:</p> <p>a. Monitors the information system to detect:</p> <ol style="list-style-type: none"> 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; <p>b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];</p> <p>c. Deploys monitoring devices:</p> <ol style="list-style-type: none"> (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; <p>d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;</p> <p>e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;</p> <p>f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and</p> <p>g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): - as needed; - [Assignment: organization-defined frequency]].</p> <p>References: None.</p>	<p>SI-4</p> <p>a. (1) sensor placement and monitoring requirements within CJCSI 6510.01F</p> <p>a. (2) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>g. (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>g. (2) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>g. (3) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-4 (4); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Inbound And Outbound Communications Traffic</p> <p>The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.</p> <p>References: None.</p>	<p>SI-4 (4) Continuously</p> <p>Source: DoD RMF TAG -----</p> <p>SI-4 (4). [continually]</p> <p>Source: FedRAMP v2 -----</p>
<p>SI-4 (5); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: System Generated Alerts</p> <p>The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].</p> <p>References: None.</p>	<p>SI-4 (5) at a minimum, the ISSM and ISSO</p> <p>Real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B</p> <p>Source: DoD RMF TAG -----</p> <p>FedRAMP Additional Requirements and Guidance: SI-4(5) Guidance: In accordance with the incident response plan.</p>

<p>SI-4 (12); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Automated Alerts</p> <p>The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined activities that trigger alerts].</p> <p>References: None.</p>	<p>SI-4 (12) When there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-4 (19); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Individuals Posing Greater Risk</p> <p>The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.</p> <p>References: None.</p>	<p>SI-4 (19) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-4 (20); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Privileged User</p> <p>The organization implements [Assignment: organization-defined additional monitoring] of privileged users.</p> <p>References: None.</p>	<p>SI-4 (20) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-4 (22); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Unauthorized Network Services</p> <p>The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection (one or more): - audits; - alerts [Assignment: organization-defined personnel or roles]].</p> <p>References: None.</p>	<p>SI-4 (22) at a minimum, the ISSM or ISSO at a minimum, the ISSM or ISSO</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-4 (23); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring - Enhancement: Host-Based Devices</p> <p>The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].</p> <p>References: NIST Special Publications 800-147, 80-155.</p>	<p>SI-4 (23) HBSS</p> <p>all components</p> <p>Source: DoD RMF TAG -----</p>

<p>SI-5; SYSTEM AND INFORMATION INTEGRITY; Security Alerts, Advisories, And Directives:</p> <p>The organization:</p> <p>a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;</p> <p>b. Generates internal security alerts, advisories, and directives as deemed necessary;</p> <p>c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): - [Assignment: organization-defined personnel or roles]; - [Assignment: organization-defined elements within the organization]; - [Assignment: organization-defined external organizations]]; and</p> <p>d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.</p> <p>References: None.</p>	<p>SI-5</p> <p>a. At a minimum, USCYBERCOM.</p> <p>c. the ISSO and ISSM</p> <p>c. not applicable as elements are not selected as recipients of security alerts, advisories and directives</p> <p>c. CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators)</p> <p>Source: DoD RMF TAG -----</p> <p>SI-5a. [to include US-CERT] SI-5c. [to include system security personnel and administrators with configuration/patch-management responsibilities]</p> <p>Source: FedRAMP v2 -----</p>
<p>SI-6; SYSTEM AND INFORMATION INTEGRITY; Security Functionality Verification:</p> <p>The information system:</p> <p>a. Verifies the correct operation of [Assignment: organization-defined security functions];</p> <p>b. Performs this verification [Selection (one or more): - [Assignment: organization-defined system transitional states]; - upon command by user with appropriate privilege; - [Assignment: organization-defined frequency]];</p> <p>c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and</p> <p>d. [Selection (one or more): - shuts the information system down; - restarts the information system; - [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.</p> <p>References: None.</p>	<p>SI-6</p> <p>a. Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>b. upon system startup, and/or restart, upon command by user with appropriate privileges</p> <p>b. 30 days</p> <p>c. the ISSO and ISSM</p> <p>d. notifies system administrator</p> <p>Source: DoD RMF TAG -----</p> <p>SI-6b [to include upon system startup and/or restart at least monthly] SI-6c [to include system administrators and security personnel] SI-6d [to include notification of system administrators and security personnel]</p> <p>Source: FedRAMP v2 -----</p>
<p>SI-7; SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring RENAMED: Software, Firmware, And Information Integrity:</p> <p>The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].</p> <p>References: None.</p>	<p>SI-7</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings.</p> <p>Source: DoD RMF TAG -----</p>

<p>SI-7 (1); SYSTEM AND INFORMATION INTEGRITY; Information System Monitoring RENAMED: Software, Firmware, And Information Integrity - Enhancement: Integrity Checks</p> <p>The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): - at startup; - at [Assignment: organization-defined transitional states or security-relevant events]; - [Assignment: organization-defined frequency]].</p> <p>References: None.</p>	<p>SI-7 (1) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Annually</p> <p>Source: DoD RMF TAG -----</p> <p>SI-7 (1). [Selection to include security relevant events and at least monthly]</p> <p>Source: FedRAMP v2 -----</p>
<p>SI-7 (7); SYSTEM AND INFORMATION INTEGRITY; Software, Firmware, And Information Integrity - Enhancement: Integration Of Detection And Response</p> <p>The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.</p> <p>References: None.</p>	<p>SI-7 (7) Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-10; SYSTEM AND INFORMATION INTEGRITY; Information Input Validation:</p> <p>The information system checks the validity of [Assignment: organization-defined information inputs].</p> <p>References: None.</p>	<p>SI-10 All inputs except those identified specifically by the organization</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-11; SYSTEM AND INFORMATION INTEGRITY; Error Handling:</p> <p>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].</p> <p>References: None.</p>	<p>SI-11 b. the ISSO, ISSM, and SCA</p> <p>Source: DoD RMF TAG -----</p>
<p>SI-16; SYSTEM AND INFORMATION INTEGRITY; Memory Protection:</p> <p>The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.</p> <p>References: None.</p>	<p>SI-16 Not appropriate for DoD to define for all CSP's infrastructure or service offerings</p> <p>Source: DoD RMF TAG -----</p>