DoD ENTERPRISE CLOUD SERVICE BROKER
CLOUD SECURITY MODEL

Version 2.1

March 13, 2014

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

Errata

The following changes have been incorporated into the Cloud Security Model, as of the date indicated in the table.

Date	**Section**	**Change**
03/13/2014	App A-E	Updated STIG/SRG tables to reflect current requirements
02/26/2014	Entire document	Edited content for minor clarifications, formatting, consistency
02/26/2014	3	Inserted concept of the DoD Cloud Sponsor to align with DoD CIO terminology
02/26/2014	4.1, 4.2, 4.3	Removed from this document; to be included in an ECSB business process document.
02/26/2014	App N	Created Appendix N; moved Appendix M Annex Section 4, Table 3 in into Appendix N
02/26/2014	App M	Moved FedRAMP controls with DoD defined parameters from Section 2, Table 1 in Appendix M Annex directly into Appendix M
02/26/2014	App A, B, C, D, E	Merged DoD controls with DoD defined parameters found in Section 2, Table in Appendix M Annex directly into Appendices A,B,C,D,E control tables as appropriate by level
02/26/2014	App A, B	Merged 1.2 and 2.0.1 into this version, 2.1, such that 2.1 now contains Levels 1-5.
12/20/2013	App K	Revised Appendix K, "Legal Matrix"
12/2/2013	Entire Document	Document revised in response to comments received during public review of v2.0 Draft and promoted to Interim Guidance status.
7/31/2013	App C, D, E	Insert Level 3, 4, 5
7/31/2013	App M	Insert Control Parameters Annex
7/19/2013	Entire Document	Corrected grammar, typos, and formatting
7/19/2013	2.1, 2.2, 4, 4.1, 4.2, 4.3, 5.1, 5.1.2, 5.2.1, 5.2.2, 5.2.3, 5.2.3.2, 5.2.4, 5.2.6, Appendices	Edited content for minor clarifications
7/19/2013	4	Added new Figure 2, "Assessment Process Flow" with introduction.

7/19/2013	4.3.7	Clarified "This Security Model provides general guidance (including a planned Appendix L, "CNDSP Addendum"), the specifics of which are ultimately within the risk acceptance of the Mission Owner with ECSB oversight."
7/19/2013	5	Revised Figure 3, "Security Model"
7/19/2013	5.2.2	Referenced emerging policy for the inclusion of NSS controls
7/19/2013	5.2.3	Revised Figure 5, DoD Ongoing Assessment and Authorization"
7/19/2013	App K	Added new Appendix K, "Legal Matrix"
7/19/2013	App L	Added new Appendix L, CNDSP Addendum" (TBP)

EXECUTIVE SUMMARY

The 26 June 2012 DoD CIO designation memo specifies that DISA will perform cloud brokerage functions to make it "easier, safer, and more productive to navigate, integrate, consume, extend and maintain cloud services, within the Department." To meet this task, DISA will focus on achieving IT efficiencies, improving reliability, interoperability, security and end-to-end performance for DoD users of cloud service offerings. DoD Components will acquire cloud services through the Enterprise Cloud Service Broker (ECSB) or obtain a waiver from the DoD CIO designated review authority (i.e., the GIG Waiver Board).

This document provides an overview of the cloud broker security process and the cloud service provider security requirements in support of the ECSB function.

Table of Contents

1 Introduction 1
1.1 Background 1
1.2 Purpose of This Document 1
2 Risk Management 1
2.1 Container Risk 1
2.2 Mission Risk 2
3 Roles and Responsibilities 2
3.1 Roles and Responsibilities 2
3.2 Security Responsibilities 3
4 Cloud Broker Security Process 4
5 Cloud Service Provider Qualification Definitions 5
5.1 Impact Levels 5
5.1.1 Max Data Type 5
5.1.2 Confidentiality, Integrity, and Availability Impact 6
5.2 Overview of Security Requirements 7
5.2.1 FedRAMP 8
5.2.2 Security Controls for National Security Systems 9
5.2.3 Ongoing Assessment 11
5.2.4 DoD Command and Control and Network Operations Integration 15
5.2.5 Architecture Integration 18
5.2.6 Policy, Guidance, Operational Constraints 18
Appendix A Impact Level 1 ..... A-1
Appendix B Impact Level 2 ..... B-1
Appendix C Impact Level 3 ..... C-1
Appendix D Impact Level 4 ..... D-1
Appendix E Impact Level 5 ..... E-1
Appendix F Impact Level 6 ..... F-1
Appendix G DoD Cloud SERVICE REQUEST Questions G-1
Appendix H DoD Cloud Customer Rule Set H-1
Appendix I References I-1
Appendix J Definitions J-1
Appendix K Legal Matrix K-1
Appendix L CNDSP Addendum L-1
Appendix M FedRAMP Security Controls with DoD Defined Control Parameters M-1
Appendix N Recommended DoD Availability Controls for Contract Consideration N-1

List of Tables

Table 1 – Roles and Responsibilities 2
Table 2 – Potential Impact Definitions for Security Objectives 7
Table 3 – Incident Categories 17
Table 4 – Impact Level 1 IaaS Additional DoD Controls Beyond FedRAMP Low A-1
Table 5 – Impact Level 1 IaaS Incident Categories A-9
Table 6 – Impact Level 1 IaaS SRGs/STIGs/Other A-11
Table 7 – Impact Level 1 PaaS Additional DoD Controls Beyond FedRAMP Low A-14
Table 8 – Impact Level 1 PaaS Incident Categories A-22
Table 9 – Impact Level 1 PaaS SRGs/STIGs/Other A-24
Table 10 – Impact Level 1 SaaS Additional DoD Controls Beyond FedRAMP Low A-28
Table 11 – Impact Level 1 SaaS Incident Categories A-36
Table 12 – Impact Level 1 SaaS SRGs/STIGs/Other A-38
Table 13 – Impact Level 2 IaaS Additional DoD Controls Beyond FedRAMP Moderate B-1
Table 14 – Impact Level 2 IaaS Incident Categories B-5
Table 15 – Impact Level 2 IaaS SRGs/STIGs/Other B-7
Table 16 – Impact Level 2 PaaS Additional DoD Controls Beyond FedRAMP Moderate B-10
Table 17 – Impact Level 2 PaaS Incident Categories B-14
Table 18 – Impact Level 2 PaaS SRGs/STIGs/Other B-16
Table 19 – Impact Level 2 SaaS Additional DoD Controls Beyond FedRAMP Moderate B-20
Table 20 – Impact Level 2 SaaS Incident Categories B-24
Table 21 – Impact Level 2 SaaS SRGs/STIGs/Other B-25
Table 22 – Impact Level 3 IaaS Additional DoD Controls Beyond FedRAMP Moderate C-1
Table 23 – Impact Level 3 IaaS Incident Categories C-6
Table 24 – Impact Level 3 IaaS SRGs/STIGs/Other C-9
Table 25 – Impact Level 3 PaaS Additional DoD Controls Beyond FedRAMP Moderate C-13
Table 26 – Impact Level 3 PaaS Incident Categories C-17
Table 27 – Impact Level 3 PaaS SRGs/STIGs/Other C-20
Table 28 – Impact Level 3 SaaS Additional DoD Controls Beyond FedRAMP Moderate C-24
Table 29 – Impact Level 3 SaaS Incident Categories C-29
Table 30 – Impact Level 3 SaaS SRGs/STIGs/Other C-31
Table 31 – Impact Level 4 IaaS Additional DoD Controls Beyond FedRAMP Moderate D-1
Table 32 – Impact Level 4 IaaS Incident Categories D-6
Table 33 – Impact Level 4 IaaS SRGs/STIGs/Other D-9
Table 34 – Impact Level 4 PaaS Additional DoD Controls Beyond FedRAMP Moderate D-12
Table 35 – Impact Level 4 PaaS Incident Categories D-17
Table 36 – Impact Level 4 PaaS SRGs/STIGs/Other D-20
Table 37 – Impact Level 4 SaaS Additional DoD Controls Beyond FedRAMP Moderate D-24
Table 38 – Impact Level 4 SaaS Incident Categories D-29
Table 39 – Impact Level 4 SaaS SRGs/STIGs/Other D-31
Table 40 – Impact Level 5 IaaS Additional DoD Controls Beyond FedRAMP Moderate E-1
Table 41 – Impact Level 5 IaaS Incident Categories E-9
Table 42 – Impact Level 5 IaaS SRGs/STIGs/Other E-11
Table 43 – Impact Level 5 PaaS Additional DoD Controls Beyond FedRAMP Moderate E-15
Table 44 – Impact Level 5 PaaS Incident Categories E-22
Table 45 – Impact Level 5 PaaS SRGs/STIGs/Other E-25

Table 46 – Impact Level 5 SaaS Additional DoD Controls Beyond FedRAMP Moderate E-28
Table 47 – Impact Level 5 SaaS Incident Categories E-36
Table 48 – Impact Level 5 SaaS SRGs/STIGs/Other E-38
Table 49 – Required System Availability G-2
Table 50 – ECSB Rule Set to Apply Against DoD Cloud Service Request Questionnaire H-1
Table 51 – Legal Matrix K-1
Table 52 – DoD Defined Control Parameters for FedRAMP Controls M-1
Table 53 – DoD Recommended Availability Controls for Contract Consideration N-1

List of Figures

Figure 1 – Notional Security Responsibilities 3
Figure 2 – Assessment Process Flow 4
Figure 3 – Security Model Overview 5
Figure 4 – FedRAMP Security Assessment Process 9
Figure 5 – DoD Ongoing Assessment and Authorization 12
Figure 6 – DoD Change Control Process 13
Figure 7 – DoD Incident Reporting and Response Coordination 15
Figure 8 – Command and Control of Computer Network Defense 18

1 Introduction

1.1 Background

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, federal data center consolidation and cloud computing efforts. Key benefits that can be achieved with cloud computing include increased mission effectiveness and operational efficiencies. Cloud computing will enable the Department to consolidate and share commodity IT functions resulting in a more efficient use of resources.

The 26 June 2012 DoD CIO designation memo specifies that the Defense Information Systems Agency (DISA) will perform cloud brokerage functions to achieve IT efficiencies, reliability, interoperability, and improve security and end-to-end performance by using cloud service offerings.

1.2 Purpose of This Document

This document establishes the DoD security requirements for cloud service providers (CSPs) to host DoD mission up to and including SECRET. Missions above SECRET must follow existing applicable DoD policies.

It is expected that the security model described in this document will continue to evolve as the ECSB learns more about DoD cloud brokering, cloud services, and cloud security through early CSP assessments and DoD cloud customer requirements.

2 Risk Management

The ECSB characterizes risk for the purposes of this document as follows. This distinction is critical to understanding the security model as it applies to container risk. Please note that, throughout the model, the terminology used is consistent with the Risk Management Framework (RMF) in order to align the ECSB processes with Federal Risk and Authorization Management Program (FedRAMP) and because the DoD is expected to sign RMF policy shortly. In the meantime, one should expect to see DoD Information Assurance Certification and Accreditation Process (DIACAP) terminology used in practice.

2.1 Container Risk

When the ECSB includes a CSP in the Enterprise Cloud Service Catalog, the ECSB is certifying and providing a DoD Provisional Authorization (PA) for the CSP to be used by a DoD cloud customer as a container. In this context, container refers to the ECSB-approved cloud service offered by a CSP, and it encompasses all DoD customer systems and data that reside in that cloud service. The DoD PA of this container certifies appropriate DoD security requirements, as defined in this document, have been and will continue to be met for the container only, and not for the overall mission in which the container will be employed. The ECSB certification and DoD PA process determines container risk only. Overall mission risk will continue to be assessed and authorized by the mission owner's Authorizing Official (AO) through the current DoD risk management process.

2.2 Mission Risk

A Mission Owner, acting as a DoD cloud customer requesting cloud services, will select an appropriate container from the Enterprise Cloud Service Catalog for its mission. That container will have been certified and provisionally authorized for DoD use by the DISA AO. The DoD cloud customer must then go through the required DoD risk management process to have its overall mission assessed and authorized but with the added benefit of having a large part of its mission, the container, already provisionally authorized by the DISA AO for DoD use. The DoD cloud customer may review all documentation associated with the DoD PA and may or may not choose to use the DoD PA as it goes through its mission authorization process. However, it is expected that, in most cases, the Mission Owner's AO will accept the DoD PA of the container to take advantage of the efficiencies inherent in that DoD PA. Specifically, since both the DoD PA and upcoming DoD authorization process are based on the RMF and share a common foundation of security controls in NIST 800-53, the DoD authorization will provide a source for inheritance of security controls. This may make the authorization process for each DoD cloud customer faster, more efficient, and shorter in duration. If a Mission Owner chooses not to accept the DoD PA, the ECSB security package will still be available to the Mission Owner to conduct an independent assessment of risk for the container. The mission authorization process determines overall mission risk and the Mission Owner's AO determines whether or not to accept the overall mission risk on behalf of the DoD. The Mission Owner maintains responsibility for complying with all DoD policy and meeting all DoD baseline requirements. In cases where the Mission Owner is following the DIACAP, they are responsible for determining how they utilize the ECSB as part of a DIACAP Certification and Accreditation (C&A).

3 Roles and Responsibilities

3.1 Roles and Responsibilities

Table 1 provides a summary of the major roles and their responsibilities in implementation of the Cloud Security Model.

Table 1 – Roles and Responsibilities

Role	Responsibility
Cloud Service Provider (CSP)	Commercial vendor or Federal organization providing cloud services
DISA Authorizing Official (AO)	Official providing PA for a CSP container for DoD use
DoD Cloud Customer	DoD entity that acquires cloud services in support of its mission
Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT)	Receiver of incident reports from CSP as mandated by the Federal Risk and Authorization Management Program (FedRAMP). Responsible for coordination across non-DoD agencies
DISA Enterprise Cloud Service Broker (ECSB)	Manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.
DoD Cloud Sponsor	Funds, acquires, and ensures Cybersecurity and contractual requirements have been met for externally provided cloud services.

Role	Responsibility
Computer Network Defense Service Provider (CNDSP)	Provider of Computer Network Defense (CND) services addressing the protection of the network, detection of threats, and response to incidents. CNDSPs provide CND at one of three tiers: Tier I (DoD-wide), Tier II (Component Level), and Tier III (Enclave Level)
DISA Field Security Operations (FSO)	Security controls assessor for CSP containers receiving PA from the DISA AO and consumer of CNDSP information.
Joint Authorization Board (JAB)	As part of FedRAMP, performs risk authorizations and grants the FedRAMP provisional ATO
Third Party Assessment Organizations (3PAO)	Within FedRAMP, perform initial and ongoing independent verification and validation of the security controls deployed within the Cloud Service Provider's information system
United States Cyber Command (USCYBERCOM)	DoD Tier I CNDSP - Notify and Coordinate as appropriate with US-CERT, Intelligence Community, Law Enforcement, and other Federal Agencies

3.2 Security Responsibilities

The ECSB responsibilities include but are not limited to providing a security model with appropriate standards, access to acquisition vehicles with appropriate terms and conditions, PAs for CSPs, and acting as the DoD customer coordinator for cloud services.

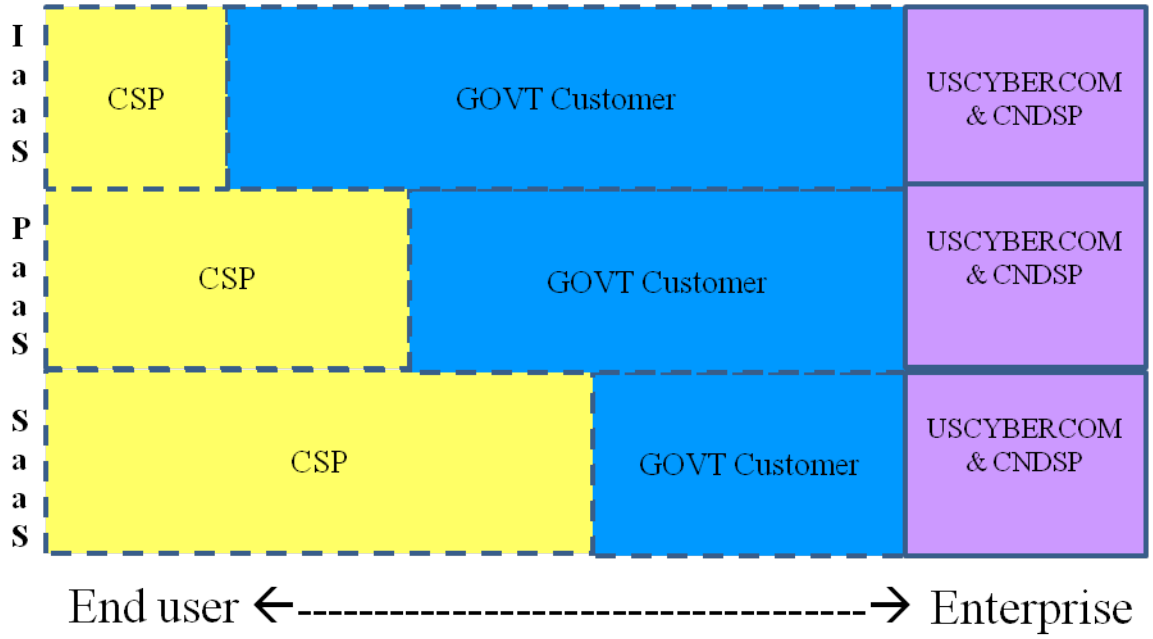

Figure 1 – Notional Security Responsibilities

For the CSP, the DoD cloud customer, and the reporting/incident handling organization(s), security responsibilities vary depending on the role and the cloud service model. Figure 1 is a notional depiction of the balance of responsibilities. The dotted lines depict that responsibilities shift to a limited degree based on many factors within the details of the security model. The

responsibilities will be clearly identified in contractual language and Service Level Agreements (SLA) as appropriate.

4 Cloud Broker Security Process

Figure 2 is a depiction of the Cloud Security Model Assessment Process Flow. It depicts how the DoD process builds on the FedRAMP CONOPS depiction.

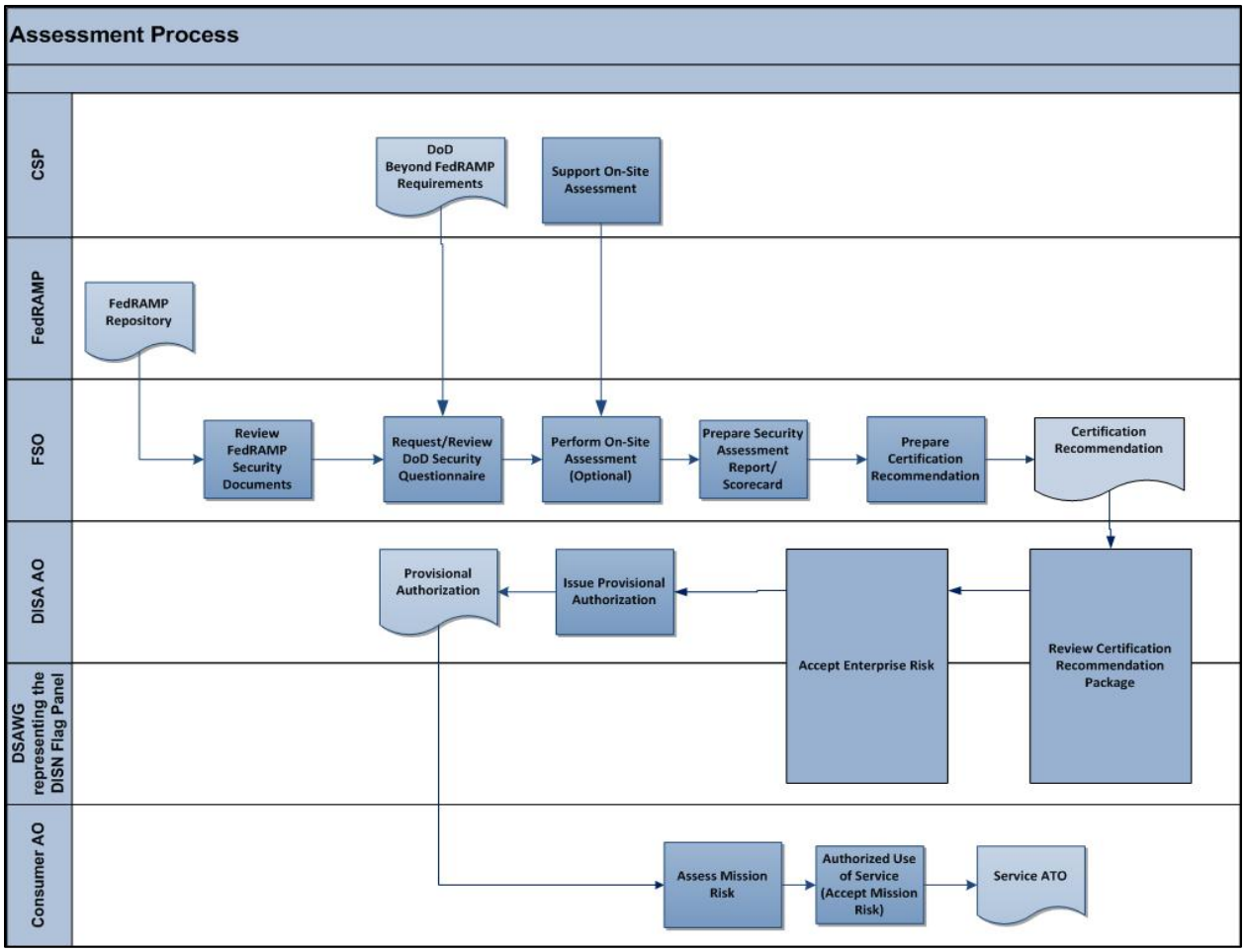

Figure 2 – Assessment Process Flow

5 Cloud Service Provider Qualification Definitions

Impact Level	Max Data Type & C-I-A	FedRAMP Secure Repository+ Federal ATO+ JAB Provisional Authorization	CNSSI 1253	Ongoing Assessment	C2 & NetOps/ CND Integration	Architectural Integration	Policy, Guidance, Operational Constraints
1	U-Public NA-L-x	L	Tailored Set with equivalency in addition to FedRAMP Low	IAW FedRAMP: 3rd party report for DoD review	IAW FedRAMP: Incident Rpts., Vulnblty Scans, POA&Ms, FedRAMP package updates, network arch updates, config updates, outage notifications; Limited bidirectional comms between CSPs & CND Tier II to include warnings and notifications	Two factor authentication for Sys Admins	Selective STIGs/SRGs/Other measures or equiv; Law Enforcement access; Official notifications; Data locations; Data spills; Data disposition; Storage Hardware disposition
2	U-Limited Access L-M-x	M	Tailored Set with equivalency in addition to FedRAMP Moderate	+ Limited ECSB assessments	+ User Level Intrusion Incidents	+ DoDI 8500.2 Passwords	+ Additional selective STIGs/SRGs/Other
3	CUI L-M-x	M	+ CUI-specific Tailored Set with equivalency	+ At least Annual 3rd party / DoD Red Teams + Red Team of significant changes	+ Non-Compliance Incidents + Rx Unclassified Threat Info + NIST ARF/ASR formats for SCM + Rx Security Policy (signatures, filters)	+ DoD PKI + DIBNet-U + NIPRnet Only	+ All STIG/CTO or equiv + DoD Community Clouds only
4	CUI M-M-x	M	Same as Level 3	Same as Level 3	+ Credible Attempt Incidents + Rx Classified Directives + Rx Classified Threat Info	+ DIBNet-S	Same as Level 3
5	CUI H-H-x	M	Tailored Set for High Impact Data with equivalency	+ As often as Quarterly 3rd party / DoD Red Teams	+ Reconnaissance Incidents	Same as Level 4	Same as Level 3
6	Classified H-H-x	M	Same as Level 5	Same as Level 5	Same as Level 5	+SIPR HW Token	+ All STIG/CTO with exception

Green: Unclassified Information not deemed CUI **Orange:** Controlled Unclassified Information **Red:** Classified up to and including Secret Information

The + sign indicates an incremental increase in requirements from the previous lower Impact Level

Figure 3 – Security Model Overview

5.1 Impact Levels

Cloud security impact levels are defined by the combination of information to be stored in the cloud 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. The ECSB has chosen six at this time, based on expectations that DoD cloud customer missions will fall into all six impact levels and that CSPs have different costs for all six impact levels. If either or both of those expectations are not realized, the ECSB will modify the impact levels by collapsing or expanding them appropriately. DoD cloud customers are expected to use the impact level that best guards against the highest impact concern for their mission/data/application. Impact levels are described further below.

5.1.1 Max Data Type

The first aspect of the security model and impact levels is the type of information to be stored or hosted in the cloud. These are as follows:

- **Public:** This refers to information that is intended for unrestricted public dissemination. This information does not require control of read access, yet does require access control with regard to access for change or delete.
- **Limited Access Information:** This refers to information that is not Controlled Unclassified Information (CUI, see below), but requires more limited access than full

public release. This data is not covered by regulations, but is data the mission owner would like to protect at their discretion using access controls.

- **Controlled Unclassified Information:** Controlled Unclassified Information (CUI) 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 categories, including, but not limited to the following:
  - Export Control--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. To include 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--Refers to personal information, or, in some cases, "personally identifiable information," as defined in Office of Management and Budget (OMB) M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7).
  - Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).
  - Other information requiring explicit CUI designation; for example, For Official Use Only, Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information.
- **Classified Information:** This is 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, the ECSB security model is considering the potential for classified, brokered cloud services only to the level of SECRET information in accordance with the applicable executive orders. Services running at higher classification levels are governed by current policies.

5.1.2 Confidentiality, Integrity, and Availability Impact

The second aspect of the security model and impact levels includes the potential impact should the confidentiality or the integrity of the information be compromised. The security model does not address the impact of availability because it is expected that the DoD cloud customer will include its availability requirements in a service level agreement with the CSP. Therefore, availability is referred to as an “x” in Figure 3. 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 the DoD Enterprise Cloud 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 DoD cloud customer, as 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 for “no single point of communications failure” then the SLA should detail “failover connection to the CSP independent of the communications path of the primary connection to the CSP.” ECSB recommended SLA availability controls are provided in Appendix N.

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 2.

Table 2 – Potential Impact Definitions for Security Objectives[1]

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

5.2 Overview of Security Requirements

The security model contains six components that address different aspects of required security. Wherever possible and appropriate, the ECSB will consider equivalencies to DoD specific security requirements provided they fully meet the intent of the security requirement as evaluated by the ECSB. It is expected that allowing for equivalencies throughout the evaluation process will minimize time and effort to get certified and maximize flexibility for CSPs to get DoD business. These components are described in the sections that follow in the context of the cloud service offerings for all impact levels, and include:

[1] FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

- FedRAMP
- Committee on National Security Systems Instruction (CNSSI) 1253 Controls
- Ongoing Assessment
- DoD Command and Control and Network Operations Integration
- Architectural Integration
- Policy, Guidance, and Operational Constraints

In general, security requirements increase within each component as the impact level increases from level 1 to level 6. Those details are found in Appendix A through Appendix F. Note that the Appendices are written as complete, stand-alone documents to allow an interested party to find all requirements for a given impact level within the applicable Appendix. Therefore, there is no attempt to avoid duplication across Appendices.

5.2.1 FedRAMP

OMB policy requires Federal departments and agencies to comply with FedRAMP guidelines by June 2014 and share Agency ATOs with the FedRAMP Secure Repository. DoD will follow this guidance for commercial cloud services. Both commercial cloud services sponsored by DoD and DoD-owned cloud services must follow OMB policy and reside in the FedRAMP Secure Repository with a FedRAMP Joint Authorization Board (JAB) PA or a U.S. Government Federal Agency ATO. DoD will honor reciprocity for the PA and accept U.S. Government Federal Agency ATOs for DoD cloud services provided the documentation resides in the FedRAMP Secure Repository.

5.2.1.1 FedRAMP Authorization

FedRAMP is a government-wide program that 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. It is the result of close collaboration with cybersecurity and cloud experts across the Federal Government and private industry. The purpose of FedRAMP is to:

- Ensure that cloud based services have adequate information security;
- Eliminate duplication of effort and reduce risk management costs; and
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies.

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

5.2.1.2 FedRAMP Security Assessment

FedRAMP PAs and Federal Agency ATOs residing in the FedRAMP Secure Repository are based on the FedRAMP security assessment process, which defines a set of controls for low and moderate impact level systems based on NIST SP 800-53 controls. The process aligns with what Federal agencies do now when assessing and authorizing cloud systems. FedRAMP uses the same documents and deliverables that NIST requires agencies to use in the SP 800-37

framework. CSPs must implement these controls and have a third party assessment organization (3PAO) perform an independent assessment of the implementation of these controls.

The FedRAMP security assessment process is compliant with FISMA and is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems.*

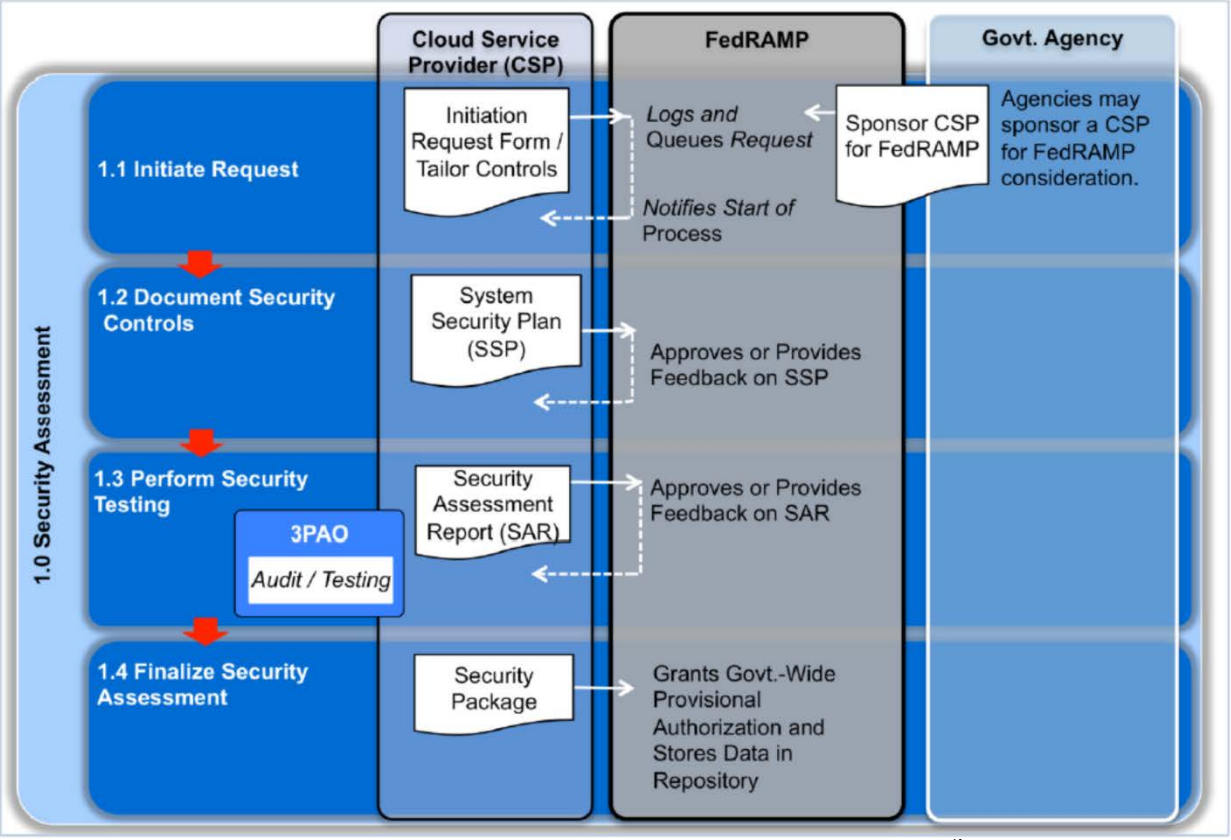

Figure 4 – FedRAMP Security Assessment Process[2]

5.2.1.3 FedRAMP Security Control Parameters

Certain NIST SP 800-53 Security Controls contain parameter values that are left to the mission to define. For those controls required by FedRAMP, the ECSB defines those parameter values in Appendix M.

5.2.2 Security Controls for National Security Systems

The Committee on National Security Systems (CNSS) worked with representatives from the Civil, Defense, and Intelligence Communities to produce a unified information security framework and to ensure NIST SP 800-53 contains security controls to meet the requirements of National Security Systems (NSS). The basis for the identification of 'national security systems' is the definition provided in law (44 U.S.C. 3542(b)(2), which was established by FISMA, Title III, Public Law 107347, December 17, 2002):

[2] FedRAMP Concept of Operation (ConOps)

> "(2)(A) The term `national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
>
> (i) the function, operation, or use of which—
> (I) involves intelligence activities;
> (II) involves cryptologic activities related to national security;
> (III) involves command and control of military forces;
> (IV) involves equipment that is an integral part of a weapon or weapons system; or
> (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
>
> (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
>
> (B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)."

Reference NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, for further information. The Director of National Intelligence and the Secretary of Defense have directed that the processes and controls described in NIST SP 800-53, as amended by CNSSI 1253, shall apply to all NSS.

Because CNSS, not NIST, has the authority to issue binding guidance for national security systems, CNSS has issued supplemental guidance for implementing NIST SP 800-53: CNSS Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, which was published in October 2009. CNSSI 1253 states that the Director of National Intelligence and the Secretary of Defense have directed that the processes described in NIST SP 800-53, revision 3 (as amended by the instruction), and the NIST security and programmatic controls contained in 800-53 apply to national security systems. Thus, CNSSI 1253 provides categorization and corresponding baseline sets of controls for national security systems. However, based on policy in the new DoDI 8510.01, all DoD Information Systems (IS) must be categorized in accordance with CNSSI 1253. One important reason for this requirement is to ensure the necessary security controls are in place so that compromise of a non-NSS connected to the Defense Information Systems Network (DISN) in any manner (e.g., an admin system connected to DoD Information Network (DoDIN)) does not lead to the compromise of another IS which may be an NSS IS, through its interconnecting network. Emerging policy also dictates the adoption of NIST processes, to include terminology.

5.2.2.1 ECSB Use of CNSSI 1253 Security Control Baselines

As described in section 5.2.2 above, all DoD systems are subject to CNSSI-1253. However, because impact levels 1 and 2 represent low-risk unclassified data, a tailored set of reduced

security controls that more closely aligns with FedRAMP will be applied to those levels. The rationale for adding controls beyond the FedRAMP baseline is twofold: 1) these controls, while not required by FedRAMP, are important to DoD because they represent controls DoD currently enforces, and 2) including these controls in the CSP qualification guidelines provides an avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The decision to add these controls explicitly considered the effectiveness of the commercial good practices being implemented by CSPs to avoid imposition of requirements that may only marginally impact the security capability already being achieved. These controls and control enhancements must be implemented and documented by the CSP and assessed by the DoD Cloud Sponsor. CSPs may offer equivalent controls, as appropriate, for consideration. For impact levels 3 through 6, a larger set of CNSSI 1253 controls apply and are tailored per each impact level definition.

5.2.2.2 CNSSI 1253 Security Control Parameters

Certain NIST SP 800-53 Security Controls contain parameter values that are left to the mission to define. For those CNSSI 1253 controls required by the DoD, the ECSB defines those parameter values in Appendix A through Appendix F.

5.2.3 Ongoing Assessment

The ECSB requires an ongoing assessment and authorization capability for CSPs providing services to the DoD. This capability, specific to DoD, is built upon the foundation of the FedRAMP continuous monitoring strategy, as described in the FedRAMP CONOPS and Continuous Monitoring Strategy & Guide. Described here is how the DoD fulfills its responsibilities within the FedRAMP Agency Role and the requirements that must be fulfilled by CSPs, specific to providing service to C/S/As within the DoD.

5.2.3.1 Operational Visibility

The DoD will review artifacts provided through the FedRAMP continuous monitoring process in addition to evidence of the implementation of any DoD-specific controls required beyond the FedRAMP controls on a continuous, ongoing basis. That information will be used in support of the annual re-authorization of each service. The dissemination of evidence for controls and the re-authorization decisions cascade through multiple levels, as reflected in Figure 5. As part of the FedRAMP process, CSPs and 3PAOs are responsible for providing deliverables attesting to the implementation of security controls. In the case of a CSP holding a FedRAMP PA, that information will be used by the FedRAMP Information System Security Officer (ISSO) to recommend to the JAB the re-authorization of the CSP for FedRAMP. In the case of a CSP holding a Federal Agency ATO without FedRAMP PA, that information will flow directly to the DoD Cloud Sponsor. The DoD will, for particular impact levels as defined above, require additional security controls. The CSP and 3PAO, as part of the CSP's continuous monitoring program, will need to supply evidence for implementation of those additional security controls. That information will flow directly to the DoD Cloud Sponsor. The DoD Cloud Sponsor will use the information received, in combination with all information provided to the FedRAMP ISSO, to recommend to the ECSB and DISA AO re-authorization of the CSP as a provisional DoD CSP. The DoD Cloud Sponsor will also provide the information to DoD cloud customers of the CSP's services. The information will be used by the relevant AOs to evaluate the risk posture of the complete system that is using the CSP's services, which may include other

services and criteria separate from the CSP, in the context of the organization's mission. That evaluation will inform the decision to provide or renew the ATO for the Mission Owner's system. The CSP will utilize mature commercial standards (e.g., comma-separated values) that fully support automated reporting.

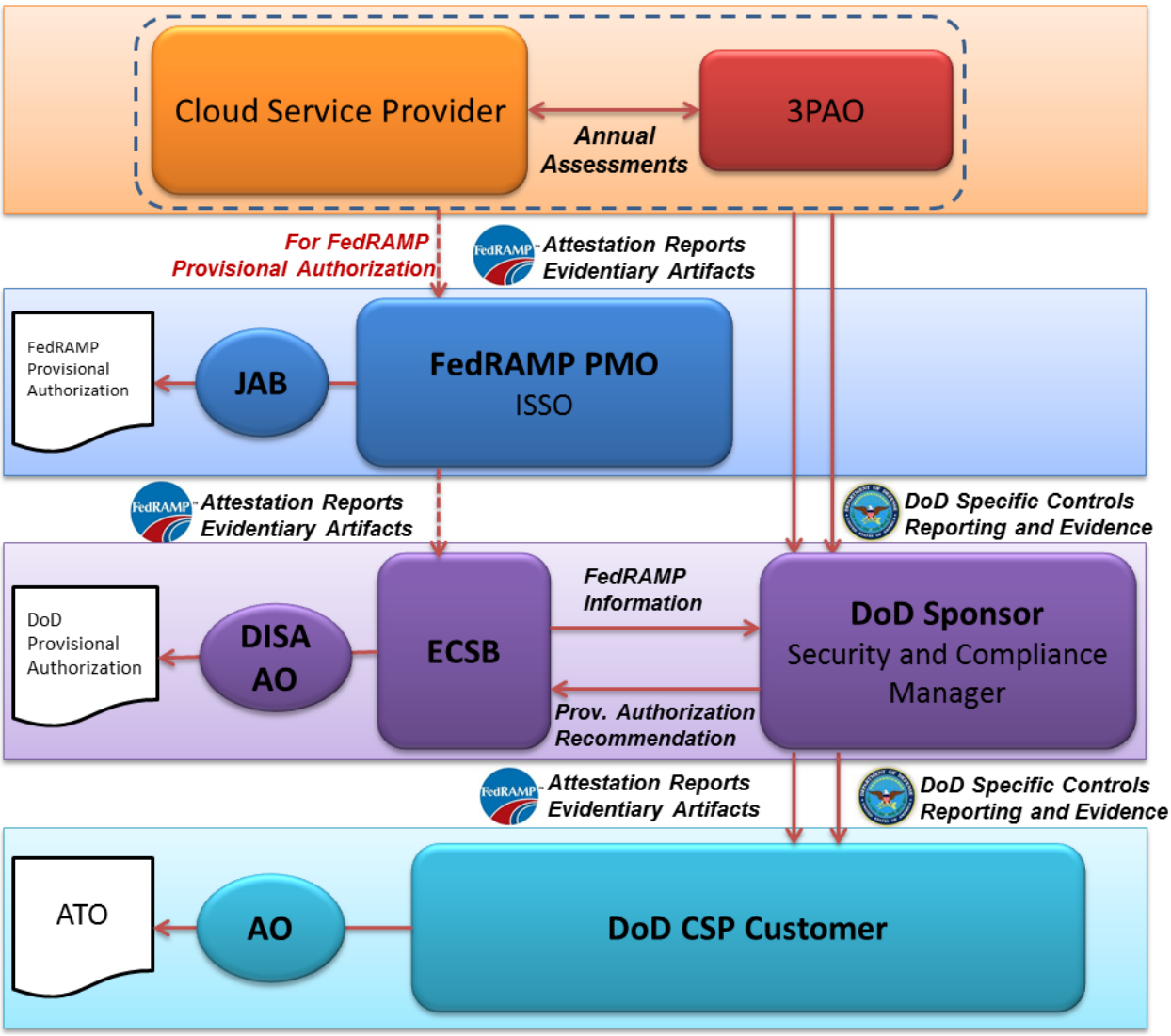

Figure 5 – DoD Ongoing Assessment and Authorization

5.2.3.2 Change Control

The DoD will review all significant changes planned by a CSP. A significant change is defined by FedRAMP and is a change to the scope of an approved PA or an impact to the authorization boundary. The FedRAMP *Significant Change Security Impact Analysis* form enumerates significant changes. The DoD will inform the assigned FedRAMP ISSO if a planned change will adversely affect the security of the information hosted by the CSP for a DoD cloud customer. The review will be performed at multiple layers, as reflected in Figure 6. 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, who will notify the ECSB, who will in turn notify the DoD Cloud Sponsor. When a CSP is included in the FedRAMP catalog, but does not have a JAB PA, the CSP will notify the DoD Cloud Sponsor directly. For CSPs in the Enterprise Cloud Service Catalog, the Security Impact Analysis must additionally cover any DoD-specific security controls required beyond the FedRAMP security controls. Once informed, the DoD Cloud Sponsor 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 organization consuming the CSP's services for any adverse impact with regard to their specific usage of the services and their specific information. In the case of a FedRAMP PA, the outcome of those reviews will be communicated back to the FedRAMP ISSO and forwarded to the JAB for their decision. Any updates to the FedRAMP Security Package will be forwarded to the ECSB.

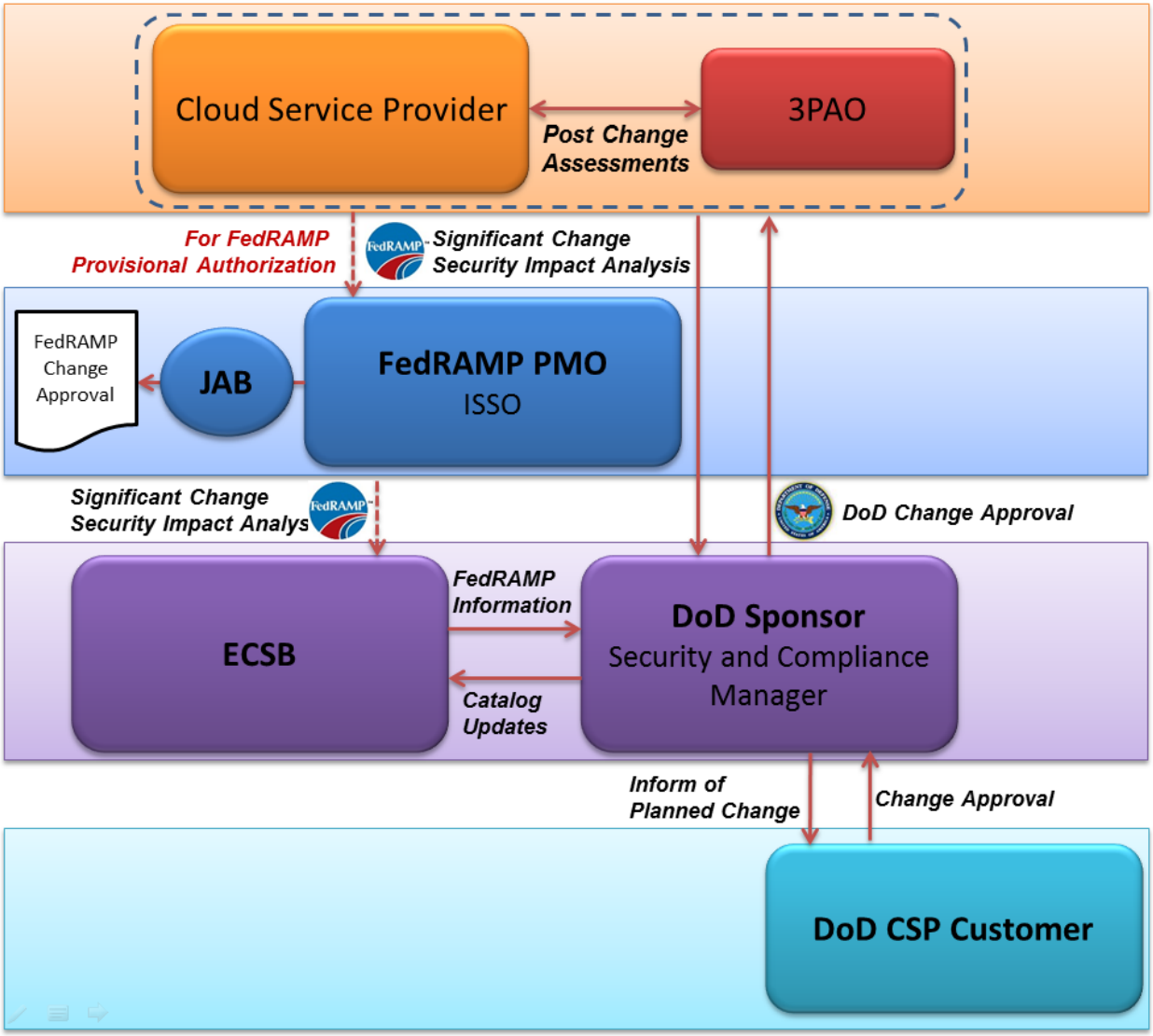

Figure 6 – DoD Change Control Process

5.2.3.3 Incident Response

The FedRAMP process requires CSPs to report incidents to US-CERT and the consuming Federal Agencies. All CSPs in the DoD Enterprise Cloud Service Catalog will be required to be supported by a DoD Computer Network Defense (CND) Tier II entity that is dedicated to CSP Operations. The CND Tier II CSP Operations entity will be the DoD Point of Contact (POC) to whom the CSP will report incidents affecting the security posture of the cloud service(s) as a container. The CSP will coordinate its response to such incidents with the CND Tier II CSP Operations entity. In addition to the CND Tier II CSP Operations entity, each DoD cloud customer of the CSP will engage the services of a Tier II CND Service Provider (CNDSP) to provide for the defense of the DoD cloud customer's mission. A DoD cloud customer's Tier II CNDSP may or may not be the same entity as the CND Tier II CSP Operations entity. DoD cloud customers will separately negotiate with the CSP the terms and requirements for incident reporting and incident response coordination with their Tier II CNDSP. For CSP services that are multi-tenant or otherwise shared across Federal Agencies outside of the DoD, incidents will be reported to US-CERT in compliance with FedRAMP requirements in parallel with the DoD reporting requirements described in this document. For CSP services that are dedicated to the DoD, incidents will not be reported to US-CERT, but only to DoD CND Tier II and DoD cloud customers. The DoD Tier I will handle coordination with US-CERT and other entities as appropriate. CSPs will effectively function as Tier III entities within the DoD structure. CSPs will provide local operational direction and support for CND and will respond to direction from their designated Tier II entity. Section 5.2.4 provides greater detail on the specific integration requirements for the CSP.

The tiered model within the DoD for Incident Reporting and Coordination is reflected in Figure 7. CSPs will report incidents, as required by their PA, by the ECSB, and by separate DoD cloud customer requirements, to all relevant Tier II entities. It is anticipated that CSPs will typically provide information directly to their DoD cloud customers regarding service availability and other measures covered under SLAs. DoD cloud customers will report availability of their systems to Tier II. This three-way information sharing provides for complete situational awareness among Tier II, DoD cloud customers, and the CSP to effectively respond to incidents. The Tier II entities will also report incidents to USCYBERCOM as required. As the Tier I, USCYBERCOM has visibility across all Tier IIs, and may notify and coordinate among them as necessary. Those other Tier II entities will, in turn, coordinate among their subscribers. USCYBERCOM will also be responsible for coordinating the DoD response with US-CERT and other entities, if that is warranted.

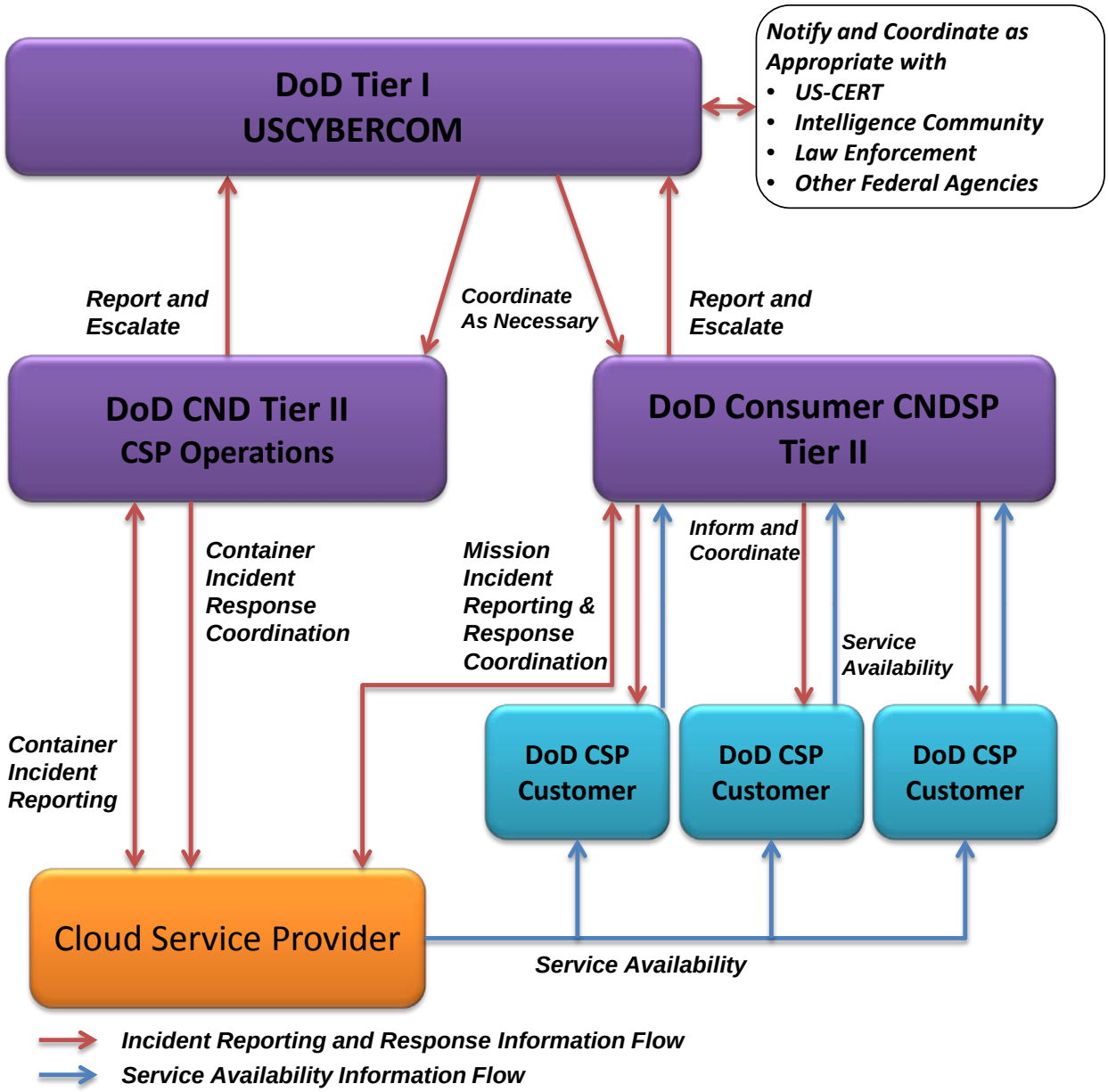

Figure 7 – DoD Incident Reporting and Response Coordination

5.2.4 DoD Command and Control and Network Operations Integration

Any provider of cloud services to the DoD will be integrated within the overall DoD Command and Control (C2) and Network Operations (NetOps) structure, to include integration with USCYBERCOM defense operations via CND Tier II. In general, the degree of integration required between a CSP and DoD C2 and NetOPs will increase with impact level. Certain requirements to integrate are beyond those specified by FedRAMP, are DoD specific implementations of FedRAMP requirements, or are DoD specific implementations of required security controls. This Security Model provides general guidance (including a planned Appendix L, "CNDSP Addendum"), the specifics of which are ultimately within the risk acceptance of the Mission Owner with ECSB awareness.

CSPs will provide an *Incident Response Plan Addendum* to document their plans for fulfilling these integration requirements. CSPs will make their plan addendum available to the ECSB for review and approval as a condition of its PA and inclusion in the Enterprise 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 Security Control Baseline (SP 800-53 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 immediate (within 60 minutes) notice to the Government of any breach of its restricted 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 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.

5.2.4.1 Information Requirements

CND Tiers I and II develop Information Requirements that identify the information necessary to accomplish their mission. CSPs are responsible for providing information (e.g., using secured email) to CND Tier II that fulfills those information requirements. In the course of performing CND for their environments, CSPs will monitor their information systems, resulting in relevant information, and report that information to the Tier II. The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type:

- Malware
- Denial of Service attack
- Targeted malicious activity
- Significant vulnerabilities
- System compromise
- Service outage with mission impact (e.g., scheduled maintenance, natural disasters)

5.2.4.2 Incident Reporting

Cloud service providers report incidents based on the current and potential impact of the incident or event on the confidentiality, availability, and integrity of organizational operations,

organizational assets, or individuals. Additionally, service providers may submit abbreviated reporting timelines to allow CND Tier II more time to collect, process, and correlate information concerning reportable events and incidents before reporting them at the national level. Follow-on reports are submitted as directed by the CND Tier II. Follow-on reports provide the raw details needed for the regional or global teams to understand the technical nature of the problem and are merged with other reports to highlight regional or global trends.

Incident categories and required reporting timelines from the CSP to CND Tier II are defined in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Appendix A to Enclosure C – Reporting Timelines. The categories of reports that are required for a CSP will vary by impact level and are documented in Appendix A to Appendix F. The incident categories are captured in Table 3.

Table 3 – Incident Categories

Incident Category	Description
1	Root Level Intrusion
2	User Level Intrusion
3	Unsuccessful Activity Attempt
4	Denial of Service
5	Non-Compliance Activity
6	Reconnaissance
7	Malicious Logic
8	Investigating
9	Explained Anomaly

5.2.4.3 Incident Reporting Mechanism

CSPs will submit reports through approved reporting mechanisms, as specified in CJCSM 6510.01B, Enclosure C, Section 4. Namely, CSPs will submit reports using the most protected means available for the affected information system. CSPs will use unclassified reporting mechanisms, such as the DoDIN, Defense Industrial Base Network (DIBNet), or non-secure phone/fax only for incidents on unclassified information systems in accordance with CJCSM 6510.01B, Enclosure C, Section 4 and Table C-1. When classified incident reporting is appropriate and directed, CSPs will use SIPRNet, DIBNet-S, or secure phone/fax to report and coordinate incidents as specified.

5.2.4.4 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 Format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting CSPs should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

5.2.4.5 Warning and Tactical Directives and Orders

The DoD operates a tiered CND 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 may be disseminated and actions directed from higher levels of command to network defenders, which include CSPs providing services to the DoD. The DoD cyber chain of command for CSPs is represented in Figure 8. USCYBERCOM, at Tier I disseminates Warnings and Tactical Directives and Orders to Tier II. The Tier II entity for CSPs will receive those items and analyze them for their applicability to individual CSPs, as well as their need-to-know. Tier II will then translate those items into instructions or security policy, which may include anti-virus and intrusion detection system/intrusion prevention system signatures, filtering policy, hostile IP lists, etc. CSPs will act as directed and implement the provided policies.

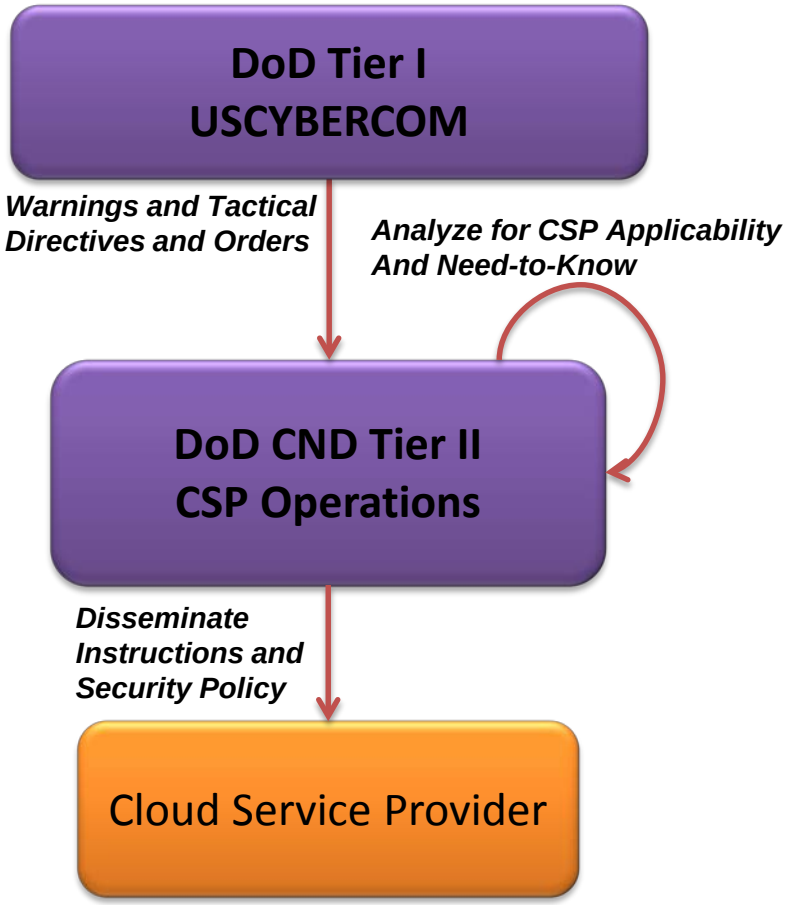

Figure 8 – Command and Control of Computer Network Defense

5.2.5 Architecture Integration

Architectural integration includes DoD specific security requirements that are above and beyond defined security controls. Specific details require more security as the impact level increases from impact level 1 to impact level 6. Those details are found in Appendix A - Appendix F.

5.2.6 Policy, Guidance, Operational Constraints

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

Appendix A Impact Level 1

A.1. Description (Unclassified-Public NA-L-x)

Loss of confidentiality of the information will have no impact, because the information has been approved for public release. Loss of integrity of the information or system will have no more than limited adverse impact since inaccurate information reaching the public may be corrected in a future information release. Loss of availability of the information will vary from none to serious adverse impact, dependent on the particular uses as specified by the DoD cloud customer.

A.2. Requirements for Infrastructure as a Service (IaaS)

A.2.1. Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 1, IaaS)

A FedRAMP Low Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

A.2.2. Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 1, IaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[3] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 4 – Impact Level 1 IaaS Additional DoD Controls Beyond FedRAMP Low

Added Control	Description
AC-6	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. (Applies to privileged access.)

[3] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel. (Applies to privileged access.)
AC-11	The information system: a. Prevents further access to the system by initiating a session lock after *[15 minutes, except to fulfill documented, AO approved and validated mission requirement]* of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. (Applies to privileged access.)
AC-11 (1)	The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. (Applies to privileged access.)
AC-17 (1)	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (Applies to privileged access.)
AC-17 (2)	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (Applies to privileged access.)
AC-17 (5)	The organization monitors for unauthorized remote connections to the information system *[continuously, real time]*, and takes appropriate action if an unauthorized connection is discovered. (Applies to privileged access.)
AU-2 (3)	The organization reviews and updates the list of auditable events *[annually or whenever there is a change in the threat environment]*. *NOTE: changes in the threat environment may be detected by the CSP and communicated to the ECSB and/or customer's CNDSP or are communicated to the service provider by the ECSB and/or customer's CNDSP in conjunction with USCYBERCOM.*
AU-2 (4)	The organization includes execution of privileged functions in the list of events to be audited by the information system.
AU-8 (1)	The information system synchronizes internal information system clocks *[at least hourly]* with *[See additional requirements and guidance. Refer to: http://tf.nist.gov/tf-cgi/servers.cgi]*. *Guidance:* *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.*

Added Control	**Description**
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-3	The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through *[See additional requirements and guidance.]* *Requirement: The service provider defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the DISA AO.* *NOTE: DoD uses the term Configuration Control Board (CCB) Alternate terms are acceptable.* that convenes [Selection: (one or more): *[See 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 DoD and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the DISA AO]*.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).

Added Control	**Description**
CM-7 (1)	The organization reviews the information system *[every 30 days]* to identify and eliminate unnecessary functions, ports, protocols, and/or services.
CM-9	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (8)	The information system uses *[See requirement]* for network access to privileged accounts. *Requirement: The service provider defines replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce). The mechanisms are approved and accepted by the DISA AO.*
IA-5 (7)	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.
IR-3	The organization tests and/or exercises the incident response capability for the information system *[annually for low/med availability systems; minimally every six months for high availability systems]* using *[The service provider provides test plans to DoD annually. Test plans are approved and accepted by the DISA AO prior to test commencing]* to determine the incident response effectiveness and documents the results.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
IR-6 (1)	The organization employs automated mechanisms to assist in the reporting of security incidents.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
RA-5 (1)	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.
RA-5 (2)	The organization updates the list of information system vulnerabilities scanned *[continuously, before each scan]* or when new vulnerabilities are identified and reported.
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.

Added Control	**Description**
SC-7 (2)	The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.
SC-7 (3)	The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.
SC-7 (4)	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy *[monthly]*; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.
SC-7 (5)	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
SC-7 (12)	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.
SC-10	The information system terminates the network connection associated with a communications session at the end of the session or after *[thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users]* of inactivity.
SC-18	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23	The information system provides mechanisms to protect the authenticity of communications sessions. (Applies to privileged access.)
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination. (Applies to privileged access.)
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages. (Applies to privileged access.)
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated. (Applies to privileged access.)

Added Control	**Description**
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*. (Applies to privileged access.)
SI-3 (1)	The organization centrally manages malicious code protection mechanisms.
SI-3 (2)	The information system automatically updates malicious code protection mechanisms (including signature definitions).
SI-3 (3)	The information system prevents non-privileged users from circumventing malicious code protection capabilities.
SI-4	The organization: a. Monitors events on the information system in accordance *[See additional requirements and guidance]* *Requirement: CSP defines monitoring objectives and processes which ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise. The monitoring objectives and processes are approved and accepted by the DISA AO.* *NOTE: DoD Sensor placement and monitoring requirements are found in CJCSI 6510.01F* and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. 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; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

Added Control	Description
SI-4 (6)	The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

A.2.3. Ongoing Assessments (Impact Level 1, IaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

A.2.4. C2 and NetOps (Impact Level 1, IaaS)

A.2.4.1. Incident Reporting (Impact Level 1, IaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 5 below. Where FedRAMP reporting refers to "agency" and "sponsoring agency", this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB.

Table 5 – Impact Level 1 IaaS Incident Categories

Incident Category	Description	Level 1 Impact	Notification Time Requirement
1	Root Level Intrusion	Low	4 Hours
4	Denial of Service	Low/Mod/High	Low: As directed by DoD Cloud Sponsor Mod/High: 15 Minutes
7	Malicious Logic	Low	As directed by DoD Cloud Sponsor

A.2.4.2. Communication with CND Tier II (Impact Level 1, IaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 1 CSPs may communicate with CND Tier II through encrypted virtual private networks (VPNs), encrypted web connections, encrypted email, or

secure phone. CSPs may communicate with CND Tier II via the Defense Industrial Base Network-Unclassified (DIBNet-U), if available, to the CSP.

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.

A.2.4.3. Vulnerability Scans (Impact Level 1, IaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

A.2.4.4. POA&Ms (Impact Level 1, IaaS)

All CSPs must send current versions of FedRAMP-required Plans of Action and Milestones (POA&Ms) to CND Tier II. CND Tier II will provide support as needed.

A.2.4.5. Warnings and Notifications (Impact Level 1, IaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

A.2.4.6. Notice of Scheduled Outages (Impact Level 1, IaaS)

All CSPs must notify CND Tier II of planned system outages in advance and provide details on planned activities during the outage.

A.2.5. Architecture Integration (Impact Level 1, IaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

A.2.5.1. Host Based Security (Impact Level 1, IaaS)

Not applicable for impact level 1.

A.2.5.2. DoD PKI (Impact Level 1, IaaS)

DoD PKI is not applicable for impact level 1. However, CSPs must provide two-factor authentication for administrative access.

A.2.5.3. Secure Communications and Collaboration Environment (Impact Level 1, IaaS)

Not applicable for Level 1.

A.2.5.4. Separation of DoD Data (Impact Level 1, IaaS)

Not applicable for Level 1.

A.2.6. Policy, Guidance, and Operational Constraints (Impact Level 1, IaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance, or operational constraints are developed.

A.2.6.1. Security Technical Implementation Guides (Impact Level 1, IaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 6 – Impact Level 1 IaaS SRGs/STIGs/Other

SRGs/STIGs/Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG

A.2.6.2. Operational Constraints (Impact Level 1, IaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

A.2.6.2.1. Law enforcement access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP

will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

A.2.6.2.2. Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

A.2.6.2.3. Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

A.2.6.2.4. Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements

A.2.6.2.5. Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

A.2.6.2.6. Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

A.2.6.3. Other Policy and Guidance (Impact Level 1, IaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

A.2.6.3.1. Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup

A.2.6.3.2. Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP

shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

A.2.6.3.3. Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

A.3. Requirements for Platform as a Service (PaaS)

A.3.1. Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 1, PaaS)

A FedRAMP Low Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

A.3.2. Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 1, PaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[4] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 7 – Impact Level 1 PaaS Additional DoD Controls Beyond FedRAMP Low

Added Control	Description

[4] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AC-6	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. (Applies to privileged access.)
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel. (Applies to privileged access.)
AC-11	The information system: a. Prevents further access to the system by initiating a session lock after *[15 minutes, except to fulfill documented, AO approved and validated mission requirement]* of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. (Applies to privileged access.)
AC-11 (1)	The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. (Applies to privileged access.)
AC-17 (1)	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (Applies to privileged access.)
AC-17 (2)	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (Applies to privileged access.)
AC-17 (5)	The organization monitors for unauthorized remote connections to the information system *[continuously, real time]* and takes appropriate action if an unauthorized connection is discovered. (Applies to privileged access.)
AU-2 (3)	The organization reviews and updates the list of auditable events *[annually or whenever there is a change in the threat environment]*. *NOTE: changes in the threat environment may be detected by the CSP and communicated to the ECSB and/or customer's CNDSP or are communicated to the service provider by the ECSB and/or customer's CNDSP in conjunction with USCYBERCOM.*
AU-2 (4)	The organization includes execution of privileged functions in the list of events to be audited by the information system.
AU-8 (1)	The information system synchronizes internal information system clocks *[at least hourly]* with *[See additional requirements and guidance. Refer to: http://tf.nist.gov/tf-cgi/servers.cgi]*. *Guidance:* *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.*

Added Control	**Description**
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-3	The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through *[See additional requirements and guidance.]* *Requirement: The service provider defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the DISA AO.* *NOTE: DoD uses the term Configuration Control Board (CCB) Alternate terms are acceptable.* that convenes [Selection: (one or more): *[See 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 DoD and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the DISA AO]*.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
CM-7 (1)	The organization reviews the information system *[every 30 days]* to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Added Control	**Description**
CM-9	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (8)	The information system uses *[See requirement]* for network access to privileged accounts. *Requirement: The service provider defines replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce). The mechanisms are approved and accepted by the DISA AO.*
IA-5 (7)	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.
IR-3	The organization tests and/or exercises the incident response capability for the information system *[annually for low/med availability systems; minimally every six months for high availability systems]* using *[The service provider provides test plans to DoD annually. Test plans are approved and accepted by the DISA AO prior to test commencing.]* to determine the incident response effectiveness and documents the results.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
IR-6 (1)	The organization employs automated mechanisms to assist in the reporting of security incidents.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
RA-5 (1)	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.
RA-5 (2)	The organization updates the list of information system vulnerabilities scanned *[continuously, before each scan]* or when new vulnerabilities are identified and reported.
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.
SC-7 (2)	The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

Added Control	**Description**
SC-7 (3)	The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.
SC-7 (4)	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy *[monthly]*; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.
SC-7 (5)	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
SC-7 (12)	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.
SC-10	The information system terminates the network connection associated with a communications session at the end of the session or after *[thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users]* of inactivity.
SC-18	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23	The information system provides mechanisms to protect the authenticity of communications sessions. (Applies to privileged access.)
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination. (Applies to privileged access.)
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages. (Applies to privileged access.)
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated. (Applies to privileged access.)

Added Control	**Description**
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*. (Applies to privileged access.)
SI-3 (1)	The organization centrally manages malicious code protection mechanisms.
SI-3 (2)	The information system automatically updates malicious code protection mechanisms (including signature definitions).
SI-3 (3)	The information system prevents non-privileged users from circumventing malicious code protection capabilities.
SI-4	The organization: a. Monitors events on the information system in accordance with *[See additional requirements and guidance]* *Requirement: CSP defines monitoring objectives and processes which ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise. The monitoring objectives and processes are approved and accepted by the DISA AO.* *NOTE: DoD Sensor placement and monitoring requirements are found in CJCSI 6510.01F* and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. 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; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.
SI-4 (6)	The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

Added Control	Description
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

A.3.3. Ongoing Assessments (Impact Level 1, PaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

A.3.4. C2 and NetOps (Impact Level 1, PaaS)

A.3.4.1. Incident Reporting (Impact Level 1, PaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Categories below. Where FedRAMP reporting refers to "agency" and "sponsoring agency", this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 8 – Impact Level 1 PaaS Incident Categories

Incident Category	Description	Level 1 Impact	Notification Time Requirement
1	Root Level Intrusion	Low	4 Hours
4	Denial of Service	Low/Mod/High	Low: As directed by DoD Cloud Sponsor Mod/High: 15 Minutes
7	Malicious Logic	Low	As directed by DoD Cloud Sponsor

A.3.4.2. Communication with CND Tier II (Impact Level 1, PaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 1 CSPs may communicate with CND Tier II through encrypted VPNs, encrypted web connections, encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

A.3.4.3. Vulnerability Scans (Impact Level 1, PaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

A.3.4.4. POA&Ms (Impact Level 1, PaaS)

All CSPs must send current versions of FedRAMP-required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

A.3.4.5. Warnings and Notifications (Impact Level 1, PaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

A.3.4.6. Notice of Scheduled Outages (Impact Level 1, PaaS)

All CSPs must notify CND Tier II of planned system outages in advance and provide details on planned activities during the outage.

A.3.5. Architecture Integration (Impact Level 1, PaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

A.3.5.1. Host Based Security (Impact Level 1, PaaS)

Not applicable for impact level 1.

A.3.5.2. DoD PKI (Impact Level 1, PaaS)

DoD PKI is not applicable for impact level 1. However, CSPs must provide two-factor authentication for administrative access.

A.3.5.3. Secure Communications and Collaboration Environment (Impact Level 1, PaaS)

Not applicable for impact level 1.

A.3.5.4. Separation of DoD Data (Impact Level 1, PaaS)

Not applicable for impact level 1.

A.3.6. Policy, Guidance, and Operational Constraints (Impact Level 1, PaaS)

This section contains DoD-specific policy, guidance, and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance, or operational constraints are developed.

A.3.6.1. Security Technical Implementation Guides (Impact Level 1, PaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 9 – Impact Level 1 PaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
Google Chrome STIG
HMC STIG
Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"

A.3.6.2. Operational Constraints (Impact Level 1, PaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

A.3.6.2.1. Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as

well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

A.3.6.2.2. Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

A.3.6.2.3. Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

A.3.6.2.4. Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency’s designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP’s continuous monitoring requirements.

A.3.6.2.5. Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

A.3.6.2.6. Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

A.3.6.3. Other Policy and Guidance (Impact Level 1, PaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

A.3.6.3.1. Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup

A.3.6.3.2. Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

A.3.6.3.3. Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

A.4. Requirements for Software as a Service (SaaS)

A.4.1. FedRAMP (Impact Level 1, SaaS)

A FedRAMP Low Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

A.4.2. Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 1, SaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[5] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls

[5] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 10 – Impact Level 1 SaaS Additional DoD Controls Beyond FedRAMP Low

Added Control	Description
AC-6	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. (Applies to privileged access.)
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel. (Applies to privileged access.)
AC-11	The information system: a. Prevents further access to the system by initiating a session lock after *[15 minutes, except to fulfill documented, AO approved and validated mission requirement]* of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. (Applies to privileged access.)
AC-11 (1)	The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. (Applies to privileged access.)
AC-17 (1)	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (Applies to privileged access.)
AC-17 (2)	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (Applies to privileged access.)
AC-17 (5)	The organization monitors for unauthorized remote connections to the information system *[continuously, real time]* and takes appropriate action if an unauthorized connection is discovered. (Applies to privileged access.)
AU-2 (3)	The organization reviews and updates the list of auditable events *[annually or whenever there is a change in the threat environment]*. *NOTE: changes in the threat environment may be detected by the CSP and communicated to the ECSB and/or customer's CNDSP or are communicated to the service provider by the ECSB and/or customer's CNDSP in conjunction with USCYBERCOM.*
AU-2 (4)	The organization includes execution of privileged functions in the list of events to be audited by the information system.

Added Control	**Description**
AU-8 (1)	The information system synchronizes internal information system clocks *[at least hourly]* with *[See additional requirements and guidance. Refer to: http://tf.nist.gov/tf-cgi/servers.cgi]*. *Guidance:* *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.*
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

Added Control	**Description**
CM-3	The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through *[See additional requirements and guidance.]* *Requirement: The service provider defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the DISA AO.* *NOTE: DoD uses the term Configuration Control Board (CCB) Alternate terms are acceptable.* that convenes [Selection: (one or more): *[See 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 DoD and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the DISA AO]*.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
CM-7 (1)	The organization reviews the information system *[every 30 days]* to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Added Control	**Description**
CM-9	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (8)	The information system uses *[See requirement]* for network access to privileged accounts. *Requirement: The service provider defines replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce). The mechanisms are approved and accepted by the DISA AO.*
IA-5 (7)	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.
IR-3	The organization tests and/or exercises the incident response capability for the information system *[annually for low/med availability systems; minimally every six months for high availability systems]* using *[The service provider provides test plans to DoD annually. Test plans are approved and accepted by the DISA AO prior to test commencing.]* to determine the incident response effectiveness and documents the results.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
IR-6 (1)	The organization employs automated mechanisms to assist in the reporting of security incidents.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
RA-5 (1)	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.
RA-5 (2)	The organization updates the list of information system vulnerabilities scanned *[continuously, before each scan]* or when new vulnerabilities are identified and reported.
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.

Added Control	**Description**
SC-7 (2)	The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.
SC-7 (3)	The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.
SC-7 (4)	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy *[monthly]*; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.
SC-7 (5)	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
SC-7 (12)	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.
SC-10	The information system terminates the network connection associated with a communications session at the end of the session or after *[thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users]* of inactivity.
SC-18	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23	The information system provides mechanisms to protect the authenticity of communications sessions. (Applies to privileged access.)
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination. (Applies to privileged access.)
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages. (Applies to privileged access.)
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated. (Applies to privileged access.)

Added Control	**Description**
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*. (Applies to privileged access.)
SI-3 (1)	The organization centrally manages malicious code protection mechanisms.
SI-3 (2)	The information system automatically updates malicious code protection mechanisms (including signature definitions).
SI-3 (3)	The information system prevents non-privileged users from circumventing malicious code protection capabilities.
SI-4	The organization: a. Monitors events on the information system in accordance with *[See additional requirements and guidance]* *Requirement: CSP defines monitoring objectives and processes which ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise. The monitoring objectives and processes are approved and accepted by the DISA AO.* *NOTE: DoD Sensor placement and monitoring requirements are found in CJCSI 6510.01F* and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. 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; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

Added Control	Description
SI-4 (6)	The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.
SI-8 (1)	The organization centrally manages spam protection mechanisms.
SI-8 (2)	The information system automatically updates spam protection mechanisms (including signature definitions).

A.4.3. Ongoing Assessments (Impact Level 1, SaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

A.4.4. C2 and NetOps (Impact Level 1, SaaS)

A.4.4.1. Incident Reporting (Impact Level 1, SaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 11 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. Impact of “Denial of Service” attacks will be based on the negotiated level of availability in the SLA.

Table 11 – Impact Level 1 SaaS Incident Categories

Incident Category	Description	Level 1 Impact	Notification Time Requirement
1	Root Level Intrusion	Low	4 Hours
4	Denial of Service	Low/Mod/High	Low: As directed by DoD Cloud Sponsor Mod/High: 15 Minutes
7	Malicious Logic	Low	As directed by DoD Cloud Sponsor

A.4.4.2. Communication with CND Tier II (Impact Level 1, SaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 1 CSPs may communicate with CND Tier II through

encrypted VPNs, encrypted web connections, encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

A.4.4.3. Vulnerability Scans (Impact Level 1, SaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

A.4.4.4. POA&Ms (Impact Level 1, SaaS)

All CSPs must send current versions of FedRAMP required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

A.4.4.5. Warnings and Notifications (Impact Level 1, SaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

A.4.4.6. Notice of Scheduled Outages (Impact Level 1, SaaS)

All CSPs must notify CND Tier II of planned system outages in advance and provide details on planned activities during the outage.

A.4.5. Architecture Integration (Impact Level 1, SaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

A.4.5.1. Host Based Security (Impact Level 1, SaaS)

Not applicable for impact level 1.

A.4.5.2. DoD PKI (Impact Level 1, SaaS)

DoD PKI is not applicable for impact level 1. However, CSPs must provide two-factor authentication for administrative access.

A.4.5.3. Secure Communications and Collaboration Environment (Impact Level 1, SaaS)

Not applicable for impact level 1.

A.4.5.4. Separation of DoD Data (Impact Level 1, SaaS)

Not applicable for impact level 1.

A.4.6. Policy, Guidance, and Operational Constraints (Impact Level 1, SaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

A.4.6.1. Security Technical Implementation Guides (Impact Level 1, SaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 12 – Impact Level 1 SaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Application Security
Application-specific STIG Documents
Desktop Application STIGs
Host Based Security System
McAfee Antivirus
Application Services
Directory Services SRG(s)/STIG(s)
Microsoft Office STIGs (Multiple versions)
Web Browser STIGs (Multiple vendors / versions)
Google Chrome STIG
Microsoft Exchange STIGs
Microsoft SharePoint 2010 STIG
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Thin Client Client (SunRay STIG)
Citrix XenApp Client STIGs
Web/App/DB Server

SRGs/STIGs/Other
Web Server SRG(s)/STIG(s) (Multiple vendors / versions)
Application Server SRG(s)/STIG(s) (Multiple vendors / versions)
Database SRG(s)/STIG(s) (Multiple vendors / versions)
.Net SRG(s)/STIG(s)
JRE SRG(s)/STIG(s)
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
Instant Messaging STIG
VVoIP STIG
VTC STIG
Enterprise Resource Planning (ERP) STIG
Enterprise System Management (ESM) STIG
HMC STIG
Other
NIST SP 800-125 “Guide to Security for Full Virtualization Technologies”

A.4.6.2. Operational Constraints (Impact Level 1, SaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

A.4.6.2.1. Law Enforcement Access (Also see Appendix K, “Legal Matrix”)

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with

the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

A.4.6.2.2. Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

A.4.6.2.3. Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

A.4.6.2.4. Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

A.4.6.2.5. Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

A.4.6.2.6. Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

A.4.6.3. Other Policy and Guidance (Impact Level 1, SaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

A.4.6.3.1. Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup

A.4.6.3.2. Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

A.4.6.3.3. Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

Appendix B Impact Level 2

B.1. Description (Unclassified-Limited Access L-M-x)

Loss of confidentiality of the information would have no more than limited adverse impact, because the information has been approved for public release but is intended for a limited public audience. Loss of integrity of the information or system will have no more than serious adverse impact since unauthorized modification or destruction of information reaching the public may be corrected in a future information release. Loss of availability of the information will vary from none to serious adverse impact, dependent on the particular uses as specified by the DoD cloud customer.

B.2. Requirements for Infrastructure as a Service (IaaS)

B.2.1. Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 2, IaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

B.2.2. Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 2, IaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[6] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 13 – Impact Level 2 IaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.

[6] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.

Added Control	**Description**
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

Added Control	Description
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

B.2.3. Ongoing Assessments (Impact Level 2, IaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

B.2.4. C2 and NetOps (Impact Level 2, IaaS)

B.2.4.1. Incident Reporting (Impact Level 2, IaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 14 below. Where FedRAMP reporting refers to "agency" and "sponsoring agency", this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 14 – Impact Level 2 IaaS Incident Categories

Incident Category	Description	Level 2 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
4	Denial of Service	Low/Mod/High	Low: As directed by DoD Sponsor Mod/High: 15 Minutes
7	Malicious Logic	Moderate	2 Hours

B.2.4.2. Communication with CND Tier II (Impact Level 2, IaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 2 CSPs may communicate with CND Tier II through encrypted VPNs, encrypted web connections, encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

B.2.4.3. Vulnerability Scans (Impact Level 2, IaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

B.2.4.4. POA&Ms (Impact Level 2, IaaS)

All CSPs must send current versions of FedRAMP required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

B.2.4.5. Warnings and Notifications (Impact Level 2, IaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

B.2.4.6. Notice of Scheduled Outages (Impact Level 2, IaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

B.2.5. Architecture Integration (Impact Level 2, IaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

B.2.5.1. Host Based Security (Impact Level 2, IaaS)

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

B.2.5.2. DoD PKI (Impact Level 2, IaaS)

DoD PKI is not applicable for impact level 2. However, CSPs must provide two-factor authentication for administrative access.

B.2.5.3. Secure Communications and Collaboration Environment (Impact Level 2, IaaS)

The secure communication channel (B.2.4.2 Communication with CND Tier II (Impact Level 2, IaaS)) will be used to convey human readable information on existing and potential threats and mitigation strategies.

B.2.5.4. Separation of DoD Data (Impact Level 2, IaaS)

Not applicable for impact level 2.

B.2.6. Policy, Guidance, and Operational Constraints (Impact Level 2, IaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

B.2.6.1. Security Technical Implementation Guides (Impact Level 2, IaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 15 – Impact Level 2 IaaS SRGs/STIGs/Other

SRGs/STIGs/Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG

B.2.6.2. Operational Constraints (Impact Level 2, IaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

B.2.6.2.1. Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP

will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

B.2.6.2.2. Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

B.2.6.2.3. Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

B.2.6.2.4. Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

B.2.6.2.5. Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

B.2.6.2.6. Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

B.2.6.3. Other Policy and Guidance (Impact Level 2, IaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

B.2.6.3.1. Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup

B.2.6.3.2. Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment within 60 days from the date of request. DoD cloud customer may also request different means of data transfer (for example, as called out in the SLA), at its discretion. After requested data is successfully transferred from CSP to DoD, CSP shall "clear" all instances of such data from its systems, in accordance with NIST 800-88.

Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

B.2.6.3.3. Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

B.3. Requirements for Platform as a Service (PaaS)

B.3.1. Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 2, PaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

B.3.2. Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 2, PaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[7] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 16 – Impact Level 2 PaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.

[7] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.

Added Control	**Description**
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

Added Control	Description
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

B.3.3. Ongoing Assessments (Impact Level 2, PaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

B.3.4. C2 and NetOps (Impact Level 2, PaaS)

B.3.4.1. Incident Reporting (Impact Level 2, PaaS)

FedRAMP requires CSPs to submit incident reports as reflect in Table 17 below. Where FedRAMP reporting refers to "agency" and "sponsoring agency", this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 17 – Impact Level 2 PaaS Incident Categories

Incident Category	Description	Level 2 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
4	Denial of Service	Low/Mod/High	Low: As directed by DoD Sponsor Mod/High: 15 Minutes
7	Malicious Logic	Moderate	2 Hours

B.3.4.2. Communication with CND Tier II (Impact Level 2, PaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 2 CSPs may communicate with CND Tier II through encrypted VPNs, encrypted web connections, encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

B.3.4.3. Vulnerability Scans (Impact Level 2, PaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

B.3.4.4. POA&Ms (Impact Level 2, PaaS)

All CSPs must send current versions of FedRAMP required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

B.3.4.5. Warnings and Notifications (Impact Level 2, PaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

B.3.4.6. Notice of Scheduled Outages (Impact Level 2, PaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

B.3.5. Architecture Integration (Impact Level 2, PaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

B.3.5.1. Host Based Security (Impact Level 2, PaaS)

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

B.3.5.2. DoD PKI (Impact Level 2, PaaS)

DoD PKI is not applicable for impact level 2. However, CSPs must provide two-factor authentication for administrative access.

B.3.5.3. Secure Communications and Collaboration Environment (Impact Level 2, PaaS)

The secure communication channel (B.3.4.2 Communication with CND Tier II (Impact Level 2, PaaS)) will be used to convey human readable information on existing and potential threats and mitigation strategies.

B.3.5.4. Separation of DoD Data (Impact Level 2, PaaS)

Not applicable for impact level 2.

B.3.6. Policy, Guidance, and Operational Constraints (Impact Level 2, PaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

B.3.6.1. Security Technical Implementation Guides (Impact Level 2, PaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 18 – Impact Level 2 PaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS **STIG**
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG
Google Chrome STIG
Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"

B.3.6.2. Operational Constraints (Impact Level 2, PaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

B.3.6.2.1. Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

B.3.6.2.2. Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

B.3.6.2.3. Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

B.3.6.2.4. Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point

of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

B.3.6.2.5. Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

B.3.6.2.6. Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

B.3.6.3. Other Policy and Guidance (Impact Level 2, PaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

B.3.6.3.1. Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.

d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
e. No hardware is destroyed or damaged as part of cleanup

B.3.6.3.2. Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

B.3.6.3.3. Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

B.4. Requirements for Software as a Service (SaaS)

B.4.1. Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 2, SaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

B.4.2. Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 2, SaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[8] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented

[8] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 19 – Impact Level 2 SaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-3 (4)	The information system enforces a Discretionary Access Control (DAC) policy that: (a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both; (b) Limits propagation of access rights; and (c) Includes or excludes access to the granularity of a single user.
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (1)	The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.

Added Control	**Description**
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.

Added Control	Description
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.
SI-8 (1)	The organization centrally manages spam protection mechanisms.
SI-8 (2)	The information system automatically updates spam protection mechanisms (including signature definitions).

B.4.3. Ongoing Assessments (Impact Level 2, SaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

B.4.4. C2 and NetOps (Impact Level 2, SaaS)

B.4.4.1. Incident Reporting (Impact Level 2, SaaS)

FedRAMP requires CSPs to submit incident reports as reflect in Table 20 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. Impact of “Denial of Service” attacks will be based on the negotiated level of availability in the SLA.

Table 20 – Impact Level 2 SaaS Incident Categories

Incident Category	Description	Level 2 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
4	Denial of Service	Low/Mod/High	Low: As directed by DoD Sponsor Mod/High: 15 Minutes
7	Malicious Logic	Moderate	2 Hours

B.4.4.2. Communication with CND Tier II (Impact Level 2, SaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 2 CSPs may communicate with CND Tier II through encrypted VPNs, encrypted web connections, encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

B.4.4.3. Vulnerability Scans (Impact Level 2, SaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

B.4.4.4. POA&Ms (Impact Level 2, SaaS)

All CSPs must send current versions of FedRAMP required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

B.4.4.5. Warnings and Notifications (Impact Level 2, SaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

B.4.4.6. Notice of Scheduled Outages (Impact Level 2, SaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

B.4.5. Architecture Integration (Impact Level 2, SaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

B.4.5.1. Host Based Security (Impact Level 2, SaaS)

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

B.4.5.2. DoD PKI (Impact Level 2, SaaS)

DoD PKI is not applicable for impact level 2. However, CSPs must provide two-factor authentication for administrative access.

B.4.5.3. Secure Communications and Collaboration Environment (Impact Level 2, SaaS)

The secure communication channel (B.4.4.2 Communication with CND Tier II (Impact Level 2, SaaS)) will be used to convey human readable information on existing and potential threats and mitigation strategies.

B.4.5.4. Separation of DoD Data (Impact Level 2, SaaS)

Not applicable for impact level 2.

B.4.6. Policy, Guidance, and Operational Constraints (Impact Level 2, SaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

B.4.6.1. Security Technical Implementation Guides (Impact Level 2, SaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 21 – Impact Level 2 SaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Application Security
Application-specific STIG Documents
Desktop Application STIGs
Host Based Security System
McAfee Antivirus
Application Services
Directory Services SRG(s)/STIG(s)
Microsoft Office STIGs (Multiple versions)

SRGs/STIGs/Other
Web Browser STIGs (Multiple vendors / versions)
Microsoft Exchange STIGs
Microsoft SharePoint 2010 STIG
Google Chrome STIG
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Thin Client Client (SunRay STIG)
Citrix XenApp Client STIGs
Web/App/DB Server
Web Server SRG(s)/STIG(s) (Multiple vendors / versions)
Application Server SRG(s)/STIG(s) (Multiple vendors / versions)
Database SRG(s)/STIG(s) (Multiple vendors / versions)
.Net SRG(s)/STIG(s)
JRE SRG(s)/STIG(s)
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG
Instant Messaging STIG
VVoIP STIG
VTC STIG
Enterprise Resource Planning (ERP) STIG
Enterprise System Management (ESM) STIG
Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"

B.4.6.2. Operational Constraints (Impact Level 2, SaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

B.4.6.2.1. Law Enforcement Access (Also see Appendix K, “Legal Matrix”)

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

B.4.6.2.2. Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

B.4.6.2.3. Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

B.4.6.2.4. Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency’s designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP’s continuous monitoring requirements.

B.4.6.2.5. Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

B.4.6.2.6. Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

B.4.6.3. Other Policy and Guidance (Impact Level 2, SaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

B.4.6.3.1. Data Spills

A “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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or “cleared” as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be “cleared” as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are “cleared” as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup

B.4.6.3.2. Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

B.4.6.3.3. Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

Appendix C Impact Level 3

C.1 Description (Controlled Unclassified Information L-M-x)

Confidentiality: The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Integrity: The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

Availability of the information will vary from none to serious adverse impact, dependent on the particular uses as specified by the DoD cloud customer.

C.2 Requirements for Infrastructure as a Service (IaaS)

C.2.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 3, IaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

C.2.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 3, IaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[9] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 22 – Impact Level 3 IaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.

[9] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan]*, *[announced]*, *[in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

Added Control	**Description**
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged.]*

Added Control	Description
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level.]*
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

C.2.3 Ongoing Assessments (Impact Level 3, IaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

C.2.4 C2 and NetOps (Impact Level 3, IaaS)

C.2.4.1 Incident Reporting (Impact Level 3, IaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 23 below. Where FedRAMP reporting refers to "agency" and "sponsoring agency", this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 23 – Impact Level 3 IaaS Incident Categories

Incident Category	Description	Level 3 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

C.2.4.2 Communication with CND Tier II (Impact Level 3, IaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 3 CSPs may communicate unclassified information with CND Tier II through DIBNet-U, encrypted VPNs, encrypted web connections, DoD PKI encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

C.2.4.3 Vulnerability Scans (Impact Level 3, IaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

C.2.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 3, IaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

C.2.4.5 Warnings and Notifications (Impact Level 3, IaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

C.2.4.6 Notice of Scheduled Outages (Impact Level 3, IaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

C.2.5 Architecture Integration (Impact Level 3, IaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

C.2.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

C.2.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available. (See IA-2 series of SP 800-53 controls)

C.2.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 3 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-U as specified by the DIB CS/IA Program.

C.2.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN Non-DoD Partner connection process, which requires consent to monitoring for all systems connected to the DoDIN. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable

boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

C.2.6 Policy, Guidance, and Operational Constraints (Impact Level 3, IaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

C.2.6.1 Security Technical Implementation Guides (Impact Level 3, IaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 24 – Impact Level 3 IaaS SRGs/STIGs/Other

SRGs/STIGs/Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG

C.2.6.2 Operational Constraints (Impact Level 3, IaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

C.2.6.2.1 Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP

will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

C.2.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

C.2.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

C.2.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

C.2.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

C.2.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

C.2.6.3 Other Policy and Guidance (Impact Level 3, IaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

C.2.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup.

C.2.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and

the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

C.2.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

C.3 Requirements for Platform as a Service (PaaS)

C.3.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 3, PaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

C.3.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 3, PaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[10] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

[10] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Table 25 – Impact Level 3 PaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan]*, *[announced]*, *[in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

Added Control	**Description**
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged.]*

Added Control	Description
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level.]*
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

C.3.3 Ongoing Assessments (Impact Level 3, PaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

C.3.4 C2 and NetOps (Impact Level 3, PaaS)

C.3.4.1 Incident Reporting (Impact Level 3, PaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 26 below. Where FedRAMP reporting refers to "agency" and "sponsoring agency", this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 26 – Impact Level 3 PaaS Incident Categories

Incident Category	Description	Level 3 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

C.3.4.2 Communication with CND Tier II (Impact Level 3, PaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 3 CSPs may communicate unclassified information with CND Tier II through DIBNet-U, encrypted VPNs, encrypted web connections, encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

C.3.4.3 Vulnerability Scans (Impact Level 3, PaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

C.3.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 3, PaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

C.3.4.5 Warnings and Notifications (Impact Level 3, PaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

C.3.4.6 Notice of Scheduled Outages (Impact Level 3, PaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

C.3.5 Architecture Integration (Impact Level 3, PaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

C.3.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

C.3.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

C.3.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 3 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-U as specified by the DIB CS/IA Program.

C.3.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable

boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

C.3.6 Policy, Guidance, and Operational Constraints (Impact Level 3, PaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

C.3.6.1 Security Technical Implementation Guides (Impact Level 3, PaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 27 – Impact Level 3 PaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG
Google Chrome STIG
Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"

C.3.6.2 Operational Constraints (Impact Level 3, PaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

C.3.6.2.1 Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

C.3.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

C.3.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

C.3.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point

of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

C.3.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

C.3.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

C.3.6.3 Other Policy and Guidance (Impact Level 3, PaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

C.3.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.

d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
e. No hardware is destroyed or damaged as part of cleanup.

C.3.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

C.3.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

C.4 Requirements for Software as a Service (SaaS)

C.4.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 3, SaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

C.4.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 3, SaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[11] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented

[11] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 28 – Impact Level 3 SaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-3 (4)	The information system enforces a Discretionary Access Control (DAC) policy that: (a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both; (b) Limits propagation of access rights; and (c) Includes or excludes access to the granularity of a single user.
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan]*, *[announced]*, *[in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (1)	The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.

Added Control	**Description**
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.
IA-5 (4)	The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.

Added Control	Description
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged.]*

Added Control	Description
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level.]*
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.
SI-8 (1)	The organization centrally manages spam protection mechanisms.
SI-8 (2)	The information system automatically updates spam protection mechanisms (including signature definitions).

C.4.3 Ongoing Assessments (Impact Level 3, SaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

C.4.4 C2 and NetOps (Impact Level 3, SaaS)

C.4.4.1 Incident Reporting (Impact Level 3, SaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 29 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of “Denial of Service” attacks will be based on the negotiated level of availability in the SLA.

Table 29 – Impact Level 3 SaaS Incident Categories

Incident Category	Description	Level 3 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

C.4.4.2 Communication with CND Tier II (Impact Level 3, SaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 3 CSPs may communicate unclassified information with CND Tier II through DIBNet-U, encrypted VPNs, encrypted web connections, DoD PKI encrypted email, or secure phone. CSPs may communicate with CND Tier II via DIBNet-U, if available, to the CSP.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

C.4.4.3 Vulnerability Scans (Impact Level 3, SaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

C.4.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 3, SaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

C.4.4.5 Warnings and Notifications (Impact Level 3, SaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

C.4.4.6 Notice of Scheduled Outages (Impact Level 3, SaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

C.4.5 Architecture Integration (Impact Level 3, SaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

C.4.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

C.4.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

C.4.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 3 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-U as specified by the DIB CS/IA Program.

C.4.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

C.4.6 Policy, Guidance, and Operational Constraints (Impact Level 3, SaaS).

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

C.4.6.1 Security Technical Implementation Guides (Impact Level 3, SaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 30 – Impact Level 3 SaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Application Security
Application-specific STIG Documents
Desktop Application STIGs
Host Based Security System
McAfee Antivirus
Application Services
Directory Services SRG(s)/STIG(s)
Microsoft Office STIGs (Multiple versions)
Web Browser STIGs (Multiple vendors / versions)
Microsoft Exchange STIGs
Microsoft SharePoint 2010 STIG
Google Chrome STIG
Domain Name Service STIG
Operating System

SRGs/STIGs/Other
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Thin Client Client (SunRay STIG)
Citrix XenApp Client STIGs
Web/App/DB Server
Web Server SRG(s)/STIG(s) (Multiple vendors / versions)
Application Server SRG(s)/STIG(s) (Multiple vendors / versions)
Database SRG(s)/STIG(s) (Multiple vendors / versions)
.Net STIG(s)
JRE STIG(s)
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG
Instant Messaging STIG
VVoIP STIG
VTC STIG
Enterprise Resource Planning (ERP) STIG
Enterprise System Management (ESM) STIG
Other
NIST SP 800-125 “Guide to Security for Full Virtualization Technologies”

C.4.6.2 Operational Constraints (Impact Level 3, SaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

C.4.6.2.1 Law Enforcement Access (Also see Appendix K, “Legal Matrix”)

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

C.4.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

C.4.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

C.4.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

C.4.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

C.4.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

C.4.6.3 Other Policy and Guidance (Impact Level 3, SaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

C.4.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup.

C.4.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and

the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

C.4.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

Appendix D Impact Level 4

D.1 Description (Controlled Unclassified Information M-M-x)

Confidentiality: The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

Integrity: The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

Availability of the information will vary from none to serious adverse impact, dependent on the particular uses as specified by the DoD cloud customer.

D.2 Requirements for Infrastructure as a Service (IaaS)

D.2.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 4, IaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

D.2.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 4, IaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[12] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 31 – Impact Level 4 IaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.

[12] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan]*, *[announced]*, *[in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

Added Control	**Description**
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged.]*.

Added Control	Description
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level.]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

D.2.3 Ongoing Assessments (Impact Level 4, IaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

D.2.4 C2 and NetOps (Impact Level 4, IaaS)

D.2.4.1 Incident Reporting (Impact Level 4, IaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 32 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of “Denial of Service” attacks will be based on the negotiated level of availability in the SLA

Table 32 – Impact Level 4 IaaS Incident Categories

Incident Category	Description	Level 4 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
3	Unsuccessful Activity Attempt	N/A	4 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

D.2.4.2 Communication with CND Tier II (Impact Level 4, IaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 4 CSPs may communicate unclassified information with CND Tier II through encrypted VPNs, encrypted web connections, DoD PKI encrypted email, or secure phone. Impact level 4 CSPs will communicate classified information with CND Tier II through DIBNet-S.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

D.2.4.3 Vulnerability Scans (Impact Level 4, IaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

D.2.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 4, IaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

D.2.4.5 Warnings and Notifications (Impact Level 4, IaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

D.2.4.6 Notice of Scheduled Outages (Impact Level 4, IaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

D.2.5 Architecture Integration (Impact Level 4, IaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

D.2.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

D.2.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

D.2.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 4 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-S as specified by the DIB CS/IA Program.

D.2.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable

boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

D.2.6 Policy, Guidance, and Operational Constraints (Impact Level 4, IaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

D.2.6.1 Security Technical Implementation Guides (Impact Level 4, IaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 33 – Impact Level 4 IaaS SRGs/STIGs/Other

SRGs/STIGs/Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG

D.2.6.2 Operational Constraints (Impact Level 4, IaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

D.2.6.2.1 Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP

will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

D.2.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

D.2.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

D.2.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

D.2.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

D.2.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

D.2.6.3 Other Policy and Guidance (Impact Level 4, IaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

D.2.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup.

D.2.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and

the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

D.2.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

D.3 Requirements for Platform as a Service (PaaS)

D.3.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 4, PaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

D.3.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 4, PaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[13] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 34 – Impact Level 4 PaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description

[13] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan]*, *[announced]*, *[in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.

Added Control	**Description**
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

Added Control	Description
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and(b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs [Selection: FIPS-validated; NSA-approved] cryptography to implement digital signatures.

Added Control	Description
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*.

Added Control	Description
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.

D.3.3 Ongoing Assessments (Impact Level 4, PaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

D.3.4 C2 and NetOps (Impact Level 4, PaaS)

D.3.4.1 Incident Reporting (Impact Level 4, PaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 35 below. Where FedRAMP reporting refers to "agency" and "sponsoring agency", this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 35 – Impact Level 4 PaaS Incident Categories

Incident Category	Description	Level 4 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
3	Unsuccessful Activity Attempt	N/A	4 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

D.3.4.2 Communication with CND Tier II (Impact Level 4, PaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 4 CSPs may communicate unclassified information with CND Tier II through encrypted VPNs, encrypted web connections, DoD PKI encrypted email, or secure phone. Impact level 4 CSPs will communicate classified information with CND Tier II through DIBNet-S.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

D.3.4.3 Vulnerability Scans (Impact Level 4, PaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

D.3.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 4, PaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed

D.3.4.5 Warnings and Notifications (Impact Level 4, PaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

D.3.4.6 Notice of Scheduled Outages (Impact Level 4, PaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

D.3.5 Architecture Integration (Impact Level 4, PaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

D.3.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

D.3.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

D.3.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 4 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-U as specified by the DIB CS/IA Program.

D.3.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable

boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

D.3.6 Policy, Guidance, and Operational Constraints (Impact Level 4, PaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

D.3.6.1 Security Technical Implementation Guides (Impact Level 4, PaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available..

Table 36 – Impact Level 4 PaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG
Google Chrome STIG
Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"

D.3.6.2 Operational Constraints (Impact Level 4, PaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

D.3.6.2.1 Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

D.3.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

D.3.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

D.3.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point

of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

D.3.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

D.3.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

D.3.6.3 Other Policy and Guidance (Impact Level 4, PaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

D.3.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.

d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
e. No hardware is destroyed or damaged as part of cleanup.

D.3.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

D.3.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

D.4 Requirements for Software as a Service (SaaS)

D.4.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 4, SaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

D.4.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 4, SaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[14] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented

[14] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 37 – Impact Level 4 SaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-3 (4)	The information system enforces a Discretionary Access Control (DAC) policy that: (a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both; (b) Limits propagation of access rights; and (c) Includes or excludes access to the granularity of a single user.
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AU-9 (4)	The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan]*, *[announced]*, *[in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-4 (1)	The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.

Added Control	**Description**
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.
IA-5 (4)	The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.

Added Control	**Description**
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged.]*.

Added Control	Description
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level.]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.
SI-8 (1)	The organization centrally manages spam protection mechanisms.
SI-8 (2)	The information system automatically updates spam protection mechanisms (including signature definitions).

D.4.3 Ongoing Assessments (Impact Level 4, SaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

D.4.4 C2 and NetOps (Impact Level 4, SaaS)

D.4.4.1 Incident Reporting (Impact Level 4, SaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 38 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of “Denial of Service” attacks will be based on the negotiated level of availability in the SLA.

Table 38 – Impact Level 4 SaaS Incident Categories

Incident Category	Description	Level 4 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
3	Unsuccessful Activity Attempt	N/A	4 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

D.4.4.2 Communication with CND Tier II (Impact Level 4, SaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 4 CSPs may communicate unclassified information with CND Tier II through encrypted VPNs, encrypted web connections, DoD PKI encrypted email, or secure phone. Impact level 4 CSPs will communicate classified information with CND Tier II through DIBNet-S.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

D.4.4.3 Vulnerability Scans (Impact Level 4, SaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

D.4.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 4, SaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

D.4.4.5 Warnings and Notifications (Impact Level 4, SaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

D.4.4.6 Notice of Scheduled Outages (Impact Level 4, SaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

D.4.5 Architecture Integration (Impact Level 4, SaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

D.4.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

D.4.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

D.4.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 4 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-U as specified by the DIB CS/IA Program.

D.4.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

D.4.6 Policy, Guidance, and Operational Constraints (Impact Level 4, SaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

D.4.6.1 Security Technical Implementation Guides (Impact Level 4, SaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 39 – Impact Level 4 SaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Application Security
Application-specific STIG Documents
Desktop Application STIGs
Host Based Security System
McAfee Antivirus
Application Services
Directory Services SRG(s)/STIG(s)
Microsoft Office STIGs (Multiple versions)
Web Browser STIGs (Multiple vendors / versions)
Microsoft Exchange STIGs
Microsoft SharePoint 2010 STIG
Google Chrome STIG
Domain Name Service STIG
Operating System

SRGs/STIGs/Other
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Thin Client Client (SunRay STIG)
Citrix XenApp Client STIGs
Web/App/DB Server
Web Server SRG(s)/STIG(s) (Multiple vendors / versions)
Application Server SRG(s)/STIG(s) (Multiple vendors / versions)
Database SRG(s)/STIG(s) (Multiple vendors / versions)
.Net STIG(s)
JRE STIG(s)
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG
Instant Messaging STIG
VVoIP STIG
VTC STIG
Enterprise Resource Planning (ERP) STIG
Enterprise System Management (ESM) STIG
Other
NIST SP 800-125 "Guide to Security for Full Virtualization Technologies"

D.4.6.2 Operational Constraints (Impact Level 4, SaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

D.4.6.2.1 Law Enforcement Access (Also see Appendix K, “Legal Matrix”)

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

D.4.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

D.4.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

D.4.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

D.4.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

D.4.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

D.4.6.3 Other Policy and Guidance (Impact Level 4, SaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

D.4.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup.

D.4.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and

the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

D.4.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

Appendix E Impact Level 5

E.1 Description (Controlled Unclassified Information H-H-x)

Confidentiality: The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Integrity: The unauthorized modification or destruction of information could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Availability of the information will vary from none to serious adverse impact, dependent on the particular uses as specified by the DoD cloud customer.

E.2 Requirements for Infrastructure as a Service (IaaS)

E.2.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 5, IaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

E.2.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 5, IaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[15] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 40 – Impact Level 5 IaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description

[15] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AC-3 (6)	The organization encrypts or stores off-line in a secure location *[Sensitive, Controlled Unclassified Information (CUI) and classified non-SAMI information]*.
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AC-6 (6)	The organization prohibits privileged access to the information system by non-organizational users.
AC-7 (1)	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
AC-9	The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).
AC-17 (6)	The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
AU-5 (1)	The information system provides a warning when allocated audit record storage volume reaches *[a maximum of 75 percent]* of maximum audit record storage capacity.
AU-5 (2)	The information system provides a real-time alert when the following audit failure events occur: *[auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded]*.
AU-9 (3)	The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.
AU-9 (4)	(a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
AU-12 (1)	The information system compiles audit records from *[All information system and network components]* into a system-wide (logical or physical) audit trail that is time-correlated to within *[200ms (two hundred milliseconds) within accreditation boundary]*
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan], [un-announced], [in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

Added Control	**Description**
CM-2 (2)	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
CM-3 (4)	The organization requires an information security representative to be a member of the *[the Configuration Control Board]*.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (2)	The organization conducts audits of information system changes *[every 7 days]* and when indications so warrant to determine whether unauthorized changes have occurred.
CM-5 (3)	The information system prevents the installation of *[patches, service packs, device drivers, and where applicable applications.]* that are not signed with a certificate that is recognized and approved by the organization.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
CM-6 (2)	The organization employs automated mechanisms to respond to unauthorized changes to *[Security related configuration settings defined at the program/system level]*.
CM-8 (2)	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.
IA-2 (4)	The information system uses multifactor authentication for local access to non-privileged accounts.
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.
IA-3 (1)	The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.
IA-3 (2)	The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Added Control	Description
IA-3 (3)	The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.
IA-5 (4)	The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.
IR-2 (1)	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
IR-6 (2)	The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
MA-4 (3)	The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.

Added Control	**Description**
MA-4 (7)	The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (1)	The organization tracks, documents, and verifies media sanitization and disposal actions.
MP-6 (2)	The organization tests sanitization equipment and procedures to verify correct performance *[every 180 days]*.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (1)	The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PE-3 (4)	The organization uses lockable physical casings to protect *[All physical components that support Virtual Machines and information storage facilities that contain DoD private CUI information having a high Confidentiality and Integrity rating (ECSB Level 5)]* from unauthorized physical access.
PE-3 (6)	The organization employs a penetration testing process that includes *[annual]*, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.
PE-8 (2)	The organization maintains a record of all physical access, both visitor and authorized individuals.

Added Control	**Description**
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-5 (4)	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.
SA-11 (2)	The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-3	The information system isolates security functions from nonsecurity functions.
SC-7 (11)	The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
SC-8 (2)	The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged.]*

Added Control	Description
SC-24	The information system fails to a *[secure state]* for *[system initialization, shutdown, and aborts]* preserving *[information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes]* in failure.
SC-28 (1)	The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.
SC-33	The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level.]*
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.
SI-7 (2)	The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

E.2.3 Ongoing Assessments (Impact Level 5, IaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

E.2.4 C2 and NetOps (Impact Level 5, IaaS)

E.2.4.1 Incident Reporting (Impact Level 5, IaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 41 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53 control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as

appropriate. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 41 – Impact Level 5 IaaS Incident Categories

Incident Category	Description	Level 5 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
3	Unsuccessful Activity Attempt	N/A	4 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
6	Reconnaissance	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

E.2.4.2 Communication with CND Tier II (Impact Level 5, IaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 5 CSPs may communicate unclassified information with CND Tier II through encrypted VPNs, encrypted web connections, DoD PKI encrypted email, or secure phone. Impact level 5 CSPs may communicate classified information with CND Tier II through DIBNet-S.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

E.2.4.3 Vulnerability Scans (Impact Level 5, IaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

E.2.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 5, IaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

E.2.4.5 Warnings and Notifications (Impact Level 5, IaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

E.2.4.6 Notice of Scheduled Outages (Impact Level 5, IaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

E.2.5 Architecture Integration (Impact Level 5, IaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

E.2.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

E.2.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

E.2.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 5 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-S as specified by the DIB CS/IA Program.

E.2.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior

approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

E.2.6 Policy, Guidance, and Operational Constraints (Impact Level 5, IaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

E.2.6.1 Security Technical Implementation Guides (Impact Level 5, IaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 42 – Impact Level 5 IaaS SRGs/STIGs/Other

SRGs/STIGs/Other
NIST SP 800-125 “Guide to Security for Full Virtualization Technologies”
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG

E.2.6.2 Operational Constraints (Impact Level 5, IaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new

DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

E.2.6.2.1 Law Enforcement Access (Also see Appendix K, "Legal Matrix")

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

E.2.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

E.2.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

E.2.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

E.2.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

E.2.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

E.2.6.3 Other Policy and Guidance (Impact Level 5, IaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

E.2.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment

b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
e. No hardware is destroyed or damaged as part of cleanup.

E.2.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

E.2.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

E.3 Requirements for Platform as a Service (PaaS)

E.3.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 5, PaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

E.3.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 5, PaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[16] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines.

[16] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 43 – Impact Level 5 PaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-3 (6)	The organization encrypts or stores off-line in a secure location *[Sensitive, Controlled Unclassified Information (CUI) and classified non-SAMI information]*.
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AC-6 (6)	The organization prohibits privileged access to the information system by non-organizational users.
AC-7 (1)	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
AC-9	The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).
AC-17 (6)	The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
AU-5 (1)	The information system provides a warning when allocated audit record storage volume reaches *[a maximum of 75 percent]* of maximum audit record storage capacity.
AU-5 (2)	The information system provides a real-time alert when the following audit failure events occur: *[auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded]*.
AU-9 (3)	The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.
AU-9 (4)	(a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.

Added Control	**Description**
AU-12 (1)	The information system compiles audit records from *[All information system and network components]* into a system-wide (logical or physical) audit trail that is time-correlated to within *[200ms (two hundred milliseconds) within accreditation boundary]*
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan]*, *[un-announced]*, *[in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-2 (2)	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
CM-3 (4)	The organization requires an information security representative to be a member of the *[the Configuration Control Board]*.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (2)	The organization conducts audits of information system changes *[every 7 days]* and when indications so warrant to determine whether unauthorized changes have occurred.
CM-5 (3)	The information system prevents the installation of *[patches, service packs, device drivers, and where applicable applications]* that are not signed with a certificate that is recognized and approved by the organization.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
CM-6 (2)	The organization employs automated mechanisms to respond to unauthorized changes to *[Security related configuration settings defined at the program/system level]*.
CM-8 (2)	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.
IA-2 (4)	The information system uses multifactor authentication for local access to non-privileged accounts.

Added Control	**Description**
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.
IA-3 (1)	The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.
IA-3 (2)	The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.
IA-3 (3)	The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.
IA-5 (4)	The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.
IR-2 (1)	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.

Added Control	**Description**
IR-6 (2)	The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
MA-4 (3)	The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MA-4 (7)	The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (1)	The organization tracks, documents, and verifies media sanitization and disposal actions.
MP-6 (2)	The organization tests sanitization equipment and procedures to verify correct performance *[every 180 days]*.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (1)	The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.

Added Control	**Description**
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PE-3 (4)	The organization uses lockable physical casings to protect *[All physical components that support Virtual Machines and information storage facilities that contain DoD private CUI information having a high Confidentiality and Integrity rating (ECSB Level 5); and/or DoD classified information (ECSB Level 6)]* from unauthorized physical access.
PE-3 (6)	The organization employs a penetration testing process that includes *[annual]*, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.
PE-8 (2)	The organization maintains a record of all physical access, both visitor and authorized individuals.
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-5 (4)	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.
SA-11 (2)	The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-3	The information system isolates security functions from nonsecurity functions.
SC-7 (11)	The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
SC-8 (2)	The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

Added Control	**Description**
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.

Added Control	Description
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*.
SC-24	The information system fails to a *[secure state]* for *[system initialization, shutdown, and aborts]* preserving *[information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes]* in failure.
SC-28 (1)	The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.
SC-33	The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.
SI-7 (2)	The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

E.3.3 Ongoing Assessments (Impact Level 5, PaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

E.3.4 C2 and NetOps (Impact Level 5, PaaS)

E.3.4.1 Incident Reporting (Impact Level 5, PaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 44 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53

control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 44 – Impact Level 5 PaaS Incident Categories

Incident Category	Description	Level 5 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
3	Unsuccessful Activity Attempt	N/A	4 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
6	Reconnaissance	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

E.3.4.2 Communication with CND Tier II (Impact Level 5, PaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 5 CSPs may communicate unclassified information with CND Tier II through DIBNet-U, encrypted VPNs, encrypted web connections, encrypted email, or secure phone. Impact level 5 CSPs may communicate classified information with CND Tier II through DIBNet-S.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

E.3.4.3 Vulnerability Scans (Impact Level 5, PaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

E.3.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 5, PaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed

E.3.4.5 Warnings and Notifications (Impact Level 5, PaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-

5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

E.3.4.6 Notice of Scheduled Outages (Impact Level 5, PaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

E.3.5 Architecture Integration (Impact Level 5, PaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

E.3.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

E.3.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

E.3.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 5 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-U as specified by the DIB CS/IA Program.

E.3.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN

Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

E.3.6 Policy, Guidance, and Operational Constraints (Impact Level 5, PaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

E.3.6.1 Security Technical Implementation Guides (Impact Level 5, PaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 45 – Impact Level 5 PaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG
Google Chrome STIG
Other
NIST SP 800-125 “Guide to Security for Full Virtualization Technologies”

E.3.6.2 Operational Constraints (Impact Level 5, PaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

E.3.6.2.1 Law Enforcement Access (Also see Appendix K, “Legal Matrix”)

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

E.3.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

E.3.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD-12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

E.3.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

E.3.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

E.3.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

E.3.6.3 Other Policy and Guidance (Impact Level 5, PaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

E.3.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup.

E.3.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

E.3.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred

to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

E.4 Requirements for Software as a Service (SaaS)

E.4.1 Federal Risk and Authorization Management Program (FedRAMP) (Impact Level 5, SaaS)

A FedRAMP Moderate Provisional Authorization (PA) / Agency Authority To Operate (ATO) is the starting point for acceptance into the Enterprise Cloud Service Catalog. For those FedRAMP controls that require parameter values, the FedRAMP defined value is acceptable for DoD unless otherwise specified in Appendix M.

E.4.2 Committee on National Security Systems Instruction (CNSSI) 1253 Controls (Impact Level 5, SaaS)

All DoD Information Systems (IS) and Platform IT (PIT) systems will be categorized in accordance with CNSSI 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are NSS or non-NSS.[17] FedRAMP also requires its own set of controls from SP 800-53 in each the low and moderate baselines. However, since FedRAMP is not subject to and does not utilize CNSSI 1253, FedRAMP baselines alone are not sufficient for DoD use. In addition, DoD policy and integration requirements necessitate controls beyond those in FedRAMP baselines. Including these controls in the CSP qualification guidelines gives us the avenue to ensure they are indeed implemented within service providers hosting DoD missions, data, and applications. The DoD Cloud Sponsor will assess these base controls and relevant related control enhancements. CSPs may offer equivalent controls, as appropriate, for consideration. For those applicable CNSSI 1253 controls that require parameter values, the ECSB defines those parameter values in italics in the table below.

Table 46 – Impact Level 5 SaaS Additional DoD Controls Beyond FedRAMP Moderate

Added Control	Description
AC-3 (4)	The information system enforces a Discretionary Access Control (DAC) policy that: a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both; (b) Limits propagation of access rights; and (c) Includes or excludes access to the granularity of a single user.
AC-3 (6)	The organization encrypts or stores off-line in a secure location *[Sensitive, Controlled Unclassified Information (CUI) and classified non-SAMI information]*.

[17] Draft DoD policy 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

Added Control	**Description**
AC-6 (5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
AC-6 (6)	The organization prohibits privileged access to the information system by non-organizational users.
AC-7 (1)	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
AC-9	The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).
AC-17 (6)	The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
AU-5 (1)	The information system provides a warning when allocated audit record storage volume reaches *[a maximum of 75 percent]* of maximum audit record storage capacity.
AU-5 (2)	The information system provides a real-time alert when the following audit failure events occur: *[auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded]*.
AU-9 (3)	The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.
AU-9 (4)	(a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
AU-12 (1)	The information system compiles audit records from *[All information system and network components]* into a system-wide (logical or physical) audit trail that is time-correlated to within *[200ms (two hundred milliseconds) within accreditation boundary]*.
CA-2 (2)	The organization includes as part of security control assessments, *[Annually or more frequently as required by the security plan], [un-announced], [in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.]*
CA-7 (1)	The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
CM-2 (2)	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Added Control	**Description**
CM-3 (4)	The organization requires an information security representative to be a member of the *[the Configuration Control Board]*.
CM-4 (1)	The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-4 (2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.
CM-5 (2)	The organization conducts audits of information system changes *[every 7 days]* and when indications so warrant to determine whether unauthorized changes have occurred.
CM-5 (3)	The information system prevents the installation of *[patches, service packs, device drivers, and where applicable applications]* that are not signed with a certificate that is recognized and approved by the organization.
CM-5 (6)	The organization limits privileges to change software resident within software libraries (including privileged programs).
CM-6 (2)	The organization employs automated mechanisms to respond to unauthorized changes to *[Security related configuration settings defined at the program/system level]*.
CM-8 (2)	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.
IA-2 (4)	The information system uses multifactor authentication for local access to non-privileged accounts.
IA-2 (5)	The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
IA-2 (9)	The information system uses *[Replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce)]* for network access to non-privileged accounts.
IA-3 (1)	The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.
IA-3 (2)	The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Added Control	Description
IA-3 (3)	The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.
IA-5 (4)	The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.
IR-2 (1)	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
IR-4 (3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. Requirement: The following are the categories of information requirements relevant to CSP operations. These information requirements are fulfilled by the CSP through incident reporting, and further detail (CJCSM 6510.01B) on reporting requirements is dependent on impact level and service type: • Malware • Denial of Service attack • Targeted malicious activity • Significant vulnerabilities • System compromise • Service outage with mission impact (e.g., scheduled maintenance, natural disasters) Requirement: The CSP defines incident categories consistent with CJCSM 6510.01B.
IR-6 (2)	The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
MA-4 (3)	The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.
MA-4 (6)	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.

Added Control	**Description**
MA-4 (7)	The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.
MP-2 (2)	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (1)	The organization tracks, documents, and verifies media sanitization and disposal actions.
MP-6 (2)	The organization tests sanitization equipment and procedures to verify correct performance *[every 180 days]*.
MP-6 (3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: *[When such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. Furthermore, USB and portable/removable drives should be system specific and not used outside of that specific system or set of systems. Once used on a system, the media must not be connected to a system that could infect it and then be reconnected to the system it supports without sanitation]*.
MP-6 (6)	The organization destroys information system media that cannot be sanitized.
PE-3 (1)	The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility
PE-3 (2)	The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.
PE-3 (3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
PE-3 (4)	The organization uses lockable physical casings to protect *[All physical components that support Virtual Machines and information storage facilities that contain DoD private CUI information having a high Confidentiality and Integrity rating (ECSB Level 5); and/or DoD classified information (ECSB Level 6)]* from unauthorized physical access.
PE-3 (6)	The organization employs a penetration testing process that includes *[annual]*, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.
PE-8 (2)	The organization maintains a record of all physical access, both visitor and authorized individuals.

Added Control	**Description**
PS-6 (1)	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.
RA-5 (4)	The organization attempts to discern what information about the information system is discoverable by adversaries.
SA-5 (4)	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.
SA-11 (2)	The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.
SA-12 (2)	The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SC-3	The information system isolates security functions from nonsecurity functions.
SC-7 (11)	The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
SC-8 (2)	The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.
SC-9 (2)	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	The organization employs *[NIST FIPS-Validated Unclassified systems]* cryptography to implement digital signatures.

Added Control	**Description**
SC-18 (2)	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets *[See additional requirements and guidance.]* *Requirement: The service provider defines a list of mobile code technologies to be deployed in information systems along with a list of specific mobile code used or planned for use; or provides a reference to source for current list. The list of mobile code and mobile code technologies is approved and accepted by DISA AO* *Requirement: Mobile code is further addressed as follows:* *(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.* *(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.* *(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.* *(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).* *(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	The information system generates unique session identifiers with *[FIPS 140-2 Approved Random Number Generators that uses the largest character set; expire and destroy session identifiers upon logout; will never be logged]*.

Added Control	Description
SC-24	The information system fails to a *[secure state]* for *[system initialization, shutdown, and aborts]* preserving *[information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes]* in failure.
SC-28 (1)	The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.
SC-33	The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.
SI-4 (1)	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	The information system notifies *[Organization defined incident response personnel (by name and/ or by role)]* of suspicious events and takes *[A list of least disruptive actions to terminate suspicious events defined at the system or program level]*.
SI-4 (8)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	The organization tests/exercises intrusion-monitoring tools *[weekly]*.
SI-7 (2)	The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.
SI-8 (1)	The organization centrally manages spam protection mechanisms.
SI-8 (2)	The information system automatically updates spam protection mechanisms (including signature definitions).

E.4.3 Ongoing Assessments (Impact Level 5, SaaS)

The CSP must comply with the ongoing assessment and authorization requirements as defined by FedRAMP. The DoD Cloud Sponsor will conduct ongoing assessments and requirements beyond FedRAMP.

E.4.4 C2 and NetOps (Impact Level 5, SaaS)

E.4.4.1 Incident Reporting (Impact Level 5, SaaS)

FedRAMP requires CSPs to submit incident reports as reflected in Table 47 below. Where FedRAMP reporting refers to “agency” and “sponsoring agency”, this corresponds to the DoD sponsor of the CSP container, which may be either DISA or another DoD entity and is separate from the DoD cloud customer. Incident categories and reporting times are in accordance with CJCSM 6510.01B. These categories are part of the implementation required by SP 800-53

control IR-4(3). DoD cloud customers will negotiate reporting requirements independent of the ECSB. CSPs will not report incidents to US-CERT, as FedRAMP dictates in certain cases. CSP will exclusively report incidents to CND Tier II, which will forward reports to other agencies as appropriate. Impact of "Denial of Service" attacks will be based on the negotiated level of availability in the SLA.

Table 47 – Impact Level 5 SaaS Incident Categories

Incident Category	Description	Level 5 Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
3	Unsuccessful Activity Attempt	N/A	4 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
6	Reconnaissance	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

E.4.4.2 Communication with CND Tier II (Impact Level 5, SaaS)

Secure bidirectional communication between CSPs and CND Tier II is essential for CSP systems to integrate with DoD CND. Impact level 5 CSPs may communicate unclassified information with CND Tier II through DIBNet-U, encrypted VPNs, encrypted web connections, DoD PKI encrypted email, or secure phone. Impact level 5 CSPs may communicate classified information with CND Tier II through DIBNet-S.

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 an level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

E.4.4.3 Vulnerability Scans (Impact Level 5, SaaS)

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CND Tier II in CSV, XML, or other approved electronic format. CND Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

E.4.4.4 Plan of Action and Milestones (POA&Ms) (Impact Level 5, SaaS)

All CSPs must send current versions of FedRAMP and ECSB required POA&Ms to CND Tier II. CND Tier II will provide support as needed.

E.4.4.5 Warnings and Notifications (Impact Level 5, SaaS)

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CND Tier II, as required by FedRAMP Security Control Baseline (SP 800-53 SI-

5). These notifications may be generated by Tier I or II CND and may include guidance for or countermeasures to be taken by CSPs.

E.4.4.6 Notice of Scheduled Outages (Impact Level 5, SaaS)

All CSPs must notify Tier II CND of planned system outages in advance and provide details on planned activities during the outage.

E.4.5 Architecture Integration (Impact Level 5, SaaS)

This section contains requirements specific to architectural integration of CSP systems with the DoD.

E.4.5.1 Host Based Security

In accordance with DoD policy, a DoD customer may install HBSS components on their systems hosted within the CSP boundary. CSPs must permit and not interfere with secure communication between Host Based Security System (HBSS) components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.

E.4.5.2 DoD PKI

CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access. 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 8520.02, and enforce the use of a physical token referred to as the "Common Access Card (CAC)" for the authentication of end 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 certificates will be used to identify applications and service contracted by the DoD. CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.

E.4.5.3 Secure Communications and Collaboration Environment

Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet and DoDIN. CSPs operating at impact level 5 are required to participate in the DIB CS/IA Program, and meet the requirements to access DIBNet-U as specified by the DIB CS/IA Program.

E.4.5.4 Separation of DoD Data

CSP systems that contain DoD data at this impact level are considered an extension of the DoDIN and will fall under the protection of the same boundary security as the rest of DoDIN. The intent is to provide separation of DoD Data from non-DoD networks and allow access to that data solely through channels that are monitored and defended by the DoD. Towards that objective, CSPs are required at this impact level to provide DoD Community Clouds with direct connection to DoDIN. To obtain those connections, CSPs are required to follow the DoDIN

Non-DoD Partner connection process, which requires consent to monitoring. Access to the cloud services from networks, such as other government networks and the public internet, may be achieved via interconnections between DoDIN and those networks, routing the traffic over the DoDIN. Any direct external connection to the cloud services other than DoDIN must gain prior approval from DISA AO. An exception to this requirement is DoD Communities of Interest who currently have approved permission to host DoD CUI Data and connect outside the DoDIN. These DoD customers will be permitted to connect to CSPs directly through their previously approved networks.

CSP systems that contain DoD data must provide appropriate separation between CSP resources ensures adequate security. Resources include any components providing compute, storage, or network. As a baseline, physical separation of resources providing DoD Community Clouds from resources supporting services for non-DoD customers is sufficient. As an example, resources dedicated for DoD use could be collocated in the same facility with non-DoD use, but DoD resources would be physically secured from access by personnel not authorized to administer DoD systems and there would be an air-gap between the DoD resources and all other resources. The DoD recognizes that CSPs may employ innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation and will consider such solutions for equivalence to physical separation. Any logical separation must provide a sufficient degree of assurance and the CSP implementation will ensure a clear, manageable boundary between the DoD data and the non-DoD data. The NSA and DISA FSO will jointly review and assess any approach involving logical separation.

E.4.6 Policy, Guidance, and Operational Constraints (Impact Level 5, SaaS)

This section contains DoD-specific policy, guidance and operational constraints and levies specific security requirements on CSPs. This section will be updated as additional policy, guidance or operational constraints are developed.

E.4.6.1 Security Technical Implementation Guides (Impact Level 5, SaaS)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. STIGs/SRGs may fulfill the baseline configuration requirement contained in the FedRAMP Security Control Baseline (SP 800-53 CM-6). STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

Table 48 – Impact Level 5 SaaS SRGs/STIGs/Other

SRGs/STIGs/Other
Application Security

SRGs/STIGs/Other
Application-specific STIG Documents
Desktop Application STIGs
Host Based Security System
McAfee Antivirus
Application Services
Directory Services SRG(s)/STIG(s)
Microsoft Office STIGs (Multiple versions)
Web Browser STIGs (Multiple vendors / versions)
Microsoft Exchange STIGs
Microsoft SharePoint 2010 STIG
Google Chrome STIG
Domain Name Service STIG
Operating System
Windows STIGs (multiple Windows versions)
UNIX SRGs & STIGs (multiple UNIX/Linux versions)
Apple OS X STIG
zOS STIG
SUSE Linux Enterprise System v11 STIG
Remote Computing
Thin Client Server (SunRay STIG)
Citrix XenApp Server STIGs
Thin Client Client (SunRay STIG)
Citrix XenApp Client STIGs
Web/App/DB Server
Web Server SRG(s)/STIG(s) (Multiple vendors / versions)
Application Server SRG(s)/STIG(s) (Multiple vendors / versions)
Database SRG(s)/STIG(s) (Multiple vendors / versions)
.Net STIG(s)
JRE STIG(s)
Other Related STIGs
VMWare ESXi 5 Server STIG
VMWare ESXi 5 vCenter Server STIG
VMWare ESXi 5 Virtual Machine STIG
HMC STIG

SRGs/STIGs/Other
Instant Messaging STIG
VVoIP STIG
VTC STIG
Enterprise Resource Planning (ERP) STIG
Enterprise System Management (ESM) STIG
Other
NIST SP 800-125 “Guide to Security for Full Virtualization Technologies”

E.4.6.2 Operational Constraints (Impact Level 5, SaaS)

The Operational Constraints set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

E.4.6.2.1 Law Enforcement Access (Also see Appendix K, “Legal Matrix”)

A CSP will provide data including meta data and web matrix monitoring for law enforcement purposes immediately upon request.

A CSP shall afford federal law enforcement agents, investigators, and auditors, including but not limited to personnel of the U.S. Department of Justice, the Offices of the various DoD Inspectors General, and the U.S. Department of Homeland Security, access to the Data Center and Data, as well as to make copies or extracts therefrom. A CSP shall segregate the Data and afford access to such information in a secure and private space, and without CSP presence, if requested.

The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, the purpose for accessing the government data, and such other data as the government may specify from time to time. The CSP will retain a copy per the records disposition schedule and will make it accessible to the agency or any other federal law enforcement, investigative, or auditing entity immediately upon request.

Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement, investigative, or auditing officials including but not limited to agency inspectors general with access to all government data to review, scan, or conduct a forensic evaluation immediately upon request without a warrant or subpoena. If government data is co-mingled with the data of another party, the CSP will isolate the government data into an environment where it may be reviewed, scanned, or forensically evaluated by Federal officials.

Note that since Government systems have a banner with consent to monitor, the Patriot Act does not apply to government data.

E.4.6.2.2 Notification

A CSP will notify the agency within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any government data. A CSP will cooperate with the agency and the

US Department of Justice to take all measures to protect the sovereignty of government data from any court, foreign, state, or local government or other legal proceeding.

E.4.6.2.3 Personnel Access

The CSP will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Agency in compliance with HSPD -12. At a minimum, all CSP employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

All employees of the CSP who have access to Government Data must sign a non-disclosure agreement.

E.4.6.2.4 Continuous Monitoring

CSP will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements.

E.4.6.2.5 Privacy Act

If the cloud service entails operation or maintenance of a Privacy Act System of Records, the Privacy Act will apply, and CSPs should note carefully and especially the provisions at 5 U.S.C. §§ 552a(i) and (m).

FAR Section 52.239-1: Privacy or Security Safeguards will apply.

E.4.6.2.6 Data Locations

A CSP will maintain all Government Data on this contract within the 50 States, the District of Columbia, and outlying areas of the United States of America. A CSP will provide the agency a list of the physical locations where the data could be stored at any given time. A CSP will update that list as new physical locations are added.

E.4.6.3 Other Policy and Guidance (Impact Level 5, SaaS)

The policy and guidance set forth below are subject to change. The DARS Council is currently processing DFARS Case 2013-D024, which should result in the issuance of a new DFARS clause or clauses related to cloud computing services contracts after the rule-making process is completed.

E.4.6.3.1 Data Spills

A "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.

Each DoD agency will provide CSP with specific response instructions. Spillage responses might generally consist of one of the following options:

1. Option 1 – Best Effort
    a. Subject data is deleted from contaminated environment.
    b. Volatile hardware with subject data will be powered down within 72 hours to clear data, subject to exceptions based on potential side effects of cleanup actions.
    c. Unencrypted subject data locations on nonvolatile storage hardware are overwritten or "cleared" as defined in NIST 800-88 within 72 hours, subject to exceptions based on potential side effects of cleanup actions.
    d. Encrypted subject data need only be deleted.
    e. No hardware is destroyed or damaged as part of cleanup.
2. Option 2 – All storage hardware involved must be "cleared" as defined in NIST 800-88
    a. Subject data is deleted from contaminated environment
    b. Volatile hardware with subject data will be powered down within 24 hours to clear data.
    c. Subject data locations on nonvolatile storage hardware are "cleared" as defined in NIST 800-88.
    d. Encrypted subject data may or may not be excepted from this, at the discretion of DoD.
    e. No hardware is destroyed or damaged as part of cleanup.

E.4.6.3.2 Disposition of Data

Upon request by a DoD cloud customer, CSP shall make all DoD cloud customer data available for electronic transfer out of CSP environment 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. If CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from CSP to DoD, CSP shall "Purge" all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline (SP 800-53 MP-6). Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.

E.4.6.3.3 Disposal of Storage Hardware

CSP shall 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 CSP and DoD, or transferred to a third party, as required by the FedRAMP Security Control Baseline (SP 800-53 MP-6). CSP shall 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.

Appendix F Impact Level 6

For the ECSB Initial Operating Capability, only DoD CSPs are eligible to provide services for impact level 6. Any DoD CSPs providing service at this impact level must have a DoD ATO.

Appendix G DoD Cloud SERVICE REQUEST Questions

1. What is the sensitivity of your data or application? Choose one.
   a. **Public information:** This refers to information that is intended for unrestricted public dissemination. This information does not require control of read access, yet does require access control with regard to access for change or delete.
   b. **Unclassified - Limited Access:** This refers to information that, while not explicitly designated as a form of Controlled Unclassified Information is deemed by the owner to be of a sensitive nature that requires additional controls or protections over public information.
   c. **Controlled Unclassified Information:** Controlled Unclassified Information (CUI) 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. CUI contains a number of categories, including following:
      a). **Export Control**--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. To include 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.
      b). **Privacy**--Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7).
      c). **Other information requiring explicit CUI designation**; for example, For Official Use Only, Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information.
   d. **Classified:** This is 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 the ECSB security model is considering the potential for classified, brokered cloud services only to the level of SECRET information in accordance with the applicable executive orders.
2. What adverse impact will the unauthorized disclosure of your data/application have on organizational operations, organizational assets, or individuals? FIPS-199 amplification included in examples for each impact level. Choose one.
   a. **NA** (Not applicable due to no impact)
   b. **Limited (Low in Table 2)** (for example, the unauthorized disclosure might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.)
   c. **Serious (Medium in Table 2)** (for example, the unauthorized disclosure might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the

functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.)

d. **Severe/catastrophic (High in Table 2)** (for example, the unauthorized disclosure might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.)

3. What adverse impact will the unauthorized modification or destruction of your data/application have on organizational operations, organizational assets, or individuals? FIPS-199 amplification included in examples for each impact level. Choose one.
   a. **Limited** (for example, the unauthorized modification or destruction might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.)
   b. **Serious** (for example, the unauthorized modification or destruction might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.)
   c. **Severe/catastrophic** (for example, the unauthorized modification or destruction might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.)
4. What level of system availability will you accept in terms of downtime over a year? (In Table 49 – Required System Availability, year is based on mean year = 365.2425 days in a year.) Choose one.

Table 49 – Required System Availability

Choice	SLA	Monthly Downtime	Annual Downtime
a	99.9%	43.8 min/mo	525.95 min/yr
b	99.95%	21.9 min/mo	262.98 min/yr
c	99.99%	4.38 min/mo	52.60 min/yr
d	99.995%	2.19 min/mo	26.30 min/yr
e	99.999%	0.44 min/mo	5.27 min /yr
f	Other, Specify		
g	Don’t Know/Depends on Cost		

5. In the event of an unplanned or unexpected service outage, what is an acceptable recovery time for your mission? Choose one.
   a. Immediate
   b. 0-2 hours

   c. 2-24 hours
   d. Other _____
   e. Don't know or depends on cost
6. Describe in a short paragraph:
   a. The type of application you require (e.g., webmail, customer relationship management, bill paying, etc.) and/or
   b. The type of application you intend to deploy and the hosting platform you require (e.g., public-facing web server with static content, public-facing web server with social networking software, etc.) and/or
   c. The type of application you intend to deploy and the hosting platform you require (e.g., parallel computing power, customer application hosted on web server, bare bones Windows or Unix virtual machine or network of machines, etc.).
7. Based on your answer to question 6, what type of Service do you require? NIST SP800-45 definitions are included. Choose one.
   a. **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
   b. **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
   c. **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which may include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Appendix H DoD Cloud Customer Rule Set

This section contains the rule set used to determine the impact level based on the DoD Cloud Service Request. The ECSB will apply the answers from questions 4-5 to help the customer establish a Service Level Agreement (SLA) with the chosen CSP.

The ECSB will use the impact level and the service type (answers from questions 6-7) to recommend cloud service options from the Enterprise Cloud Service Catalog to the DoD cloud customer. If there are no cloud service offerings in the catalog for the impact level required, the ECSB will use the next highest (i.e., more secure) impact level.

Table 50 – ECSB Rule Set to Apply Against DoD Cloud Service Request Questionnaire

Question 1 (Data Sensitivity)	Question 2 (Confidentiality)	Question 3 (Integrity)	Impact Level
Unclassified - Public	NA	L	1
Unclassified - Public	NA	M	2
Unclassified - Public	NA	H	5
Unclassified - Public	L	L	1
Unclassified - Public	L	M	2
Unclassified - Public	L	H	5
Unclassified - Public	M	L	2
Unclassified - Public	M	M	4
Unclassified - Public	M	H	5
Unclassified - Public	H	L or M or H	5
Unclassified - Limited Access	L	L	1
Unclassified - Limited Access	L	M	2
Unclassified - Limited Access	L	H	5
Unclassified - Limited Access	M	L	4
Unclassified - Limited Access	M	M	4
Unclassified - Limited Access	M	H	5
Unclassified - Limited Access	H	L or M or H	5
CUI	L	L	3
CUI	L	M	3
CUI	L	H	5
CUI	M	L	4
CUI	M	M	4
CUI	M	H	5
CUI	H	L or M or H	5
Classified	L* or M or H	L or M or H	6

Note: L* is intended to be comprehensive allowing the Mission Owner to protect “need to know” information. See also Table 2 – Potential Impact Definitions for Security Objectives.

Appendix I 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 15 March 2012.
   http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf
3. CNSSI 4009: National Information Assurance (IA) Glossary, dated 26 April 2010.
   http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
4. Executive Order 13526: Classified National Security Information, dated 29 December 2009.
   http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information
5. DoD Chief Information Officer, Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker, dated 26 June 2012.
   http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/disa-designation-memo.pdf
6. DoD Chief Information Officer, Interim Guidance Memorandum on Use of Commercial Cloud Computing Services, dated 9 December 2011.
   http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/Intermin%20Guidance%20Memo%20on%20Use%20of%20Commerical%20Cloud%20Computing%20Services.pdf
7. DoD Instructions, 8500 Series.
   http://www.dtic.mil/whs/directives/corres/ins1.html
   Note: the 8500 Series is currently in revision. The ECSB team used both the current instructions and the new, under review, instructions as appropriate. The Series includes 8500, 8510.01, 8520, etc.
8. Defense Information Systems Agency, DoD Enterprise Cloud Service Broker website.
   http://disa.mil/Services/DoD-Cloud-Broker
9. Defense Information Systems Agency, DoD Enterprise Cloud Service Broker Security Model Controls Parameters, in draft.
10. FedRAMP: The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
    http://cloud.cio.gov/fedramp
11. FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.
    http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
12. NIST SP 500-292: NIST Cloud Computing Reference Architecture, dated September 2011.
    http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

13. NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, dated August 2009.
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/800-53-rev3_markup-rev2-to-rev3_updated-may-01-2010.pdf

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

14. 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

15. 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

16. 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

17. 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

18. 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

19. 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

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

Appendix J 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: per NIST, 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

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

Container: The ECSB-approved cloud service offered by a CSP, encompassing all customer systems and data that reside in that cloud service.

DoD Community 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 sufficient separation from resources not dedicated to DoD use.

Infrastructure as a Service (IaaS): Infrastructure 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): Platform includes execution runtime, database, web server, development tools, etc.

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

Restricted Data: sensitive data, not available to the public but not classified.

Software as a Service (SaaS): Software includes Email, virtual desktop, communication, applications, etc.

Unrestricted Data: Public facing, publically available data.

Appendix K Legal Matrix

The Legal Matrix provides a crosswalk between the Legal Rationale and the Cloud Security Model guidance.

The crosswalk legend follows:

A – All (legal guidance that applies to all areas)

S – Software (legal guidance that is specific to software)

C – Controlled Unclassified and Classified Data (legal guidance that is specific to Controlled Unclassified and Classified Data)

Table 51 – Legal Matrix

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
1	Inspector General Act of 1978 (IGA) Federal Information Security Management Act of 2002 (FISMA) NIST 800-53	PHYSICAL ACCESS DoD agencies require physical access to CSP data centers to conduct inspections under FISMA, for audit purposes, and Inspector General investigations. Such inspections, audits, and investigations may be unannounced, so DoD agencies must ensure that its inspectors, auditors, and investigators have the access required complete their inspections, audits, and investigations.	A	1-6
2	Homeland Security Presidential Directive No. 12 (HSPD-12)	PERSONNEL ACCESS DoD agencies must require that all CSP employees who have access to Government data, or the physical and logical architecture that supports Government data, be U.S. persons per Executive Order 12333 and pass an appropriate background check as required by HSPD-12	A	1-6

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
3	Freedom of Information Act (FOIA) Unless there is a "consultant" relationship (*Department of Interior v. Klamath*) Government information falls under the "release to one release to all" rule (*NARA v. Favish*), which would prevent the Government from refusing to release non-public (e.g., FOUO) information if the same information was released to a contractor without an NDA.	NON-DISCLOSURE AGREEMENT (NDA) DoD agencies must require that CSP employees with access to non-public Government data and information sign an NDA that would legally prohibit a CSP employee from disclosing non-public Government data and information.	A	1-6
4	Asset availability procedures	ASSET AVAILABILITY DoD agencies should ensure that the service level agreement with the CSP contains provision for asset availability. The level of asset availability will be determined by agency requirements.	A	1-6
5	4th Amendment Banner language establishes constructive consent for the Government to view content and monitor activity on a Government system without a warrant (*City of Ontario v. Quon*).	BANNER Banners or consent to monitor language allows Federal law enforcement the right to access and review Government data, including email created on a Government system, without a warrant or a subpoena. When DoD agencies acquire hosting services, banner language will be a requirement of the system developer. When acquiring software as a service, however, DoD agencies must require that the CSP display the agencies' approved banner language prior to allowing a user access to the system.	S	1-6

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
6	The Procurement Integrity Act (41 U.S.C. §§ 2101-2107) (PIA); FAR 3.104; and FAR subpart 9.5, Organizational and Consultant Conflicts of Interest (OCI)	PIA and OCI When DoD agencies places commercial proprietary information, contractor bid or proposal information, source selection information, or non-public information on a commercial cloud, the agencies must ensure that the CSP refrains from using or releasing such information in violation of the cited legal authorities. Special NDAs are required to avoid or mitigate OCI.	C	3-6
7	FISMA DoD agencies are responsible for accepting the risk for an IT system.	CONTINUOUS MONITORING FedRAMP mandates certain requirements for continuous monitoring in the "Continuous Mentoring Strategy Guide". These requirements require the CSP to produce certain reports and provide them to FedRAMP PMO and/or a FedRAMP 3PAO. DoD agencies need to request copies of these reports as deliverables (PWS/SOW), as the DoD Designated Authorizing Authority is ultimately responsible for the protection of the data.	A	1-6
8	FISMA; OMB Memorandum M-07-16, May 22, 2007 (safeguarding and responding to breaches of personally identifiable information (PII); and 44 U.S.C. §§ 3544(b)(7) and 3546 (reports to the United States-Computer Emergency Readiness	DATA BREACH and PII To mitigate the risk of a data breach, DoD agencies must require that CSPs provide a plan for handling such a breach which includes the requirement to notify the agency of a breach within 60 minutes (a US-CERT requirement). In addition, DoD agencies are required to conduct a Privacy Impact Assessment (PIA) on all of their IT systems. The purpose of the PIA is to analyze how information in identifiable form is handled;	C	3-6

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
	Team (US-CERT), within the Department of Homeland Security. (*See also*, section 208 of the E-Government Act of 2002, and OMB Memorandum M-03-22.)	to ensure that its handling conforms to applicable legal, regulatory, and policy requirements for privacy; to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and to examine and evaluate protections and alternative processes for handling such information to mitigate potential privacy risks. To assist an agency in developing the PIA, the CSP must be required to provide the agency with any required data about the CSP environment.		
9	IGA; FISMA	FACILITY INSPECTIONS FISMA and DoD policy require that facilities hosting DoD data meet certain security standards. Routine inspections ensure that facilities are in compliance with these standards. Usually these inspections are conducted by the Government; however, in the case of a CSP the Government may agree to allow a third party to conduct an inspection based on the Government's criteria.	A	1-6
10	FISMA	COMPLIANCE When hosting Government data, CSPs must comply with FISMA and related agency policies.	A	1-6
11	Privity of Contract	USE OF SUBCONTRACTORS When subcontracting, the agency should ensure that the prime contractor retains operational configuration and control of Government data.	A	1-6

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
12	Sovereign Immunity	INDEMNIFICATION Indemnification by the CSP benefits the Government when third parties make claims or sue the Government when the CSP, and not the Government, is liable. Indemnification allows the Government to avoid or recoup costs related to a third-party law suit.	A	1-6
13	General Liability	INSURANCE DoD agencies must require that CSPs have the necessary insurance to cover costs stemming from a breach of Government data or damage to a DoD system.	A	1-6
14	Data Sovereignty	JURISDICTION Government data must not reside within a foreign jurisdiction due to the risk that such data might be seized by a foreign Government or other non-U.S. authorities.	A	1-6
15	IGA; FISMA; and general law enforcement authorities	LAW ENFORCEMENT As mentioned above, all users of DoD systems have constructively consented through the banner language to monitoring of their use of a DoD system and use of that data for law enforcement purposes. As such, Federal law enforcement, investigative, and auditing officials do not need a warrant or a subpoena to access Government data on a Government system.	A	1-6

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
16	FISMA	VULNERABILITY SECURITY MAINTANCE Agencies must require CSPs to conduct regular maintenance including patches on its environment to prevent intrusions.	A	1-6
17	Sovereign Immunity	NOTIFICATION CSP data centers are subject to state and local authorities, and state and local legal process (e.g., subpoenas). The Agency must ensure the CSP notifies the agency of a warrant or a subpoena to take action to protect Government data from unauthorized release.	A	1-6
18	Federal Records Act and FOIA	RECORDS DoD agencies are required to maintain and produce records per the Federal Records Act, the Freedom of Information Act, and the Federal Rules of Civil Procedure. Records are kept based on the Agency's disposition schedule. The Government should work with the CSP to ensure that all Government records and CSP records about Government data are kept in accordance with Agency record's schedules.	A	1-6
19	CNSS 1001	SPILLAGE When classified information "spills over" to an unclassified system happens, DoD agencies must ensure that CSPs follow the procedures in CNSS 1001.	A	1-6

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
20	HSPD 23; NSPD 54; Sec. 806, NDAA 2011; and DoDI 5200.44	SUPPLY CHAIN RISK MANAGEMENT The Agency must ensure that CSPs exercise due diligence to use genuine hardware and software products that are free of malware.	C	3-6
21	A number of different laws and legal concepts are implicated when commercial terms of service (TOS) agreements are involved, to wit: FOIA Anti-Deficiency Act	TERMS OF SERVICE (TOS) Many commercial services have TOS Agreements that contain clauses that the Government cannot accept. Below are some examples: **CONFIDENTIALITY** This is a clause where the Government agrees not to release confidential information. However, the Government is subject to the Freedom of Information Act and must follow its procedures to release or protect commercial information. **INDEMNIFICATION** Many terms of service agreement contain an open ended indemnification clause where the Government will indemnify the CSP against third party claims. This type of clause violates the Anti-Deficiency Act because the Government is committing to funds that have yet to be appropriated. This clause needs to be re-worked to reference other applicable laws.	A	1-6

#	Legal Reference or Concept	Description of Issue and Solution	Crosswalk	Applicable ECSB Impact Levels
	Sovereign Immunity 5 C.F.R. 2635.702; FAR 3.101-1; and E.O. 12731	**GOVERNING LAW** Many TOS agreements specify the governing law and venue for adjudicating disputes. Disputes involving the Federal Government can only be adjudicated in accordance with Federal law. **ENDORSEMENTS** Many TOS agreements have a clause given the CSP the right to quote or cite the Government's use of the CSP's product as an endorsement. The Government does not normally endorse commercial products or services.		

Appendix L CNDSP Addendum

To Be Published

Appendix M FedRAMP Security Controls with DoD Defined Control Parameters

Appendix M is comprised of those FedRAMP required controls where DoD defines the values for the control parameters. In the case of FedRAMP required controls with no DoD defined parameter value, DoD requires the FedRAMP value which can be found in FedRAMP documentation.

In Table 52, for those security controls where a degree of flexibility is provided by allowing organizations to define input values for certain parameters associated with the controls, the control listed under "Short Control Verbiage Highlighting the Variable/Parameter" has the format [*Assignment: organization-defined element*]. The associated DoD-defined security control parameter value is listed under "DoD Control Parameter Requirements (Values/Selections)" and has the format "Parameter: [*value*]", where the information in square brackets replaces the "*Assignment: organization-defined element*]" content.

Table 52 – DoD Defined Control Parameters for FedRAMP Controls

Short Control Verbiage Highlighting the Variable/Parameter	DoD Control Parameter Requirements (Values/Selections)
Access Controls	
AC-2; Account Management: The organization manages information system accounts, including: … j. Reviewing accounts *[Assignment: organization-defined frequency]*.	AC-2 j. Parameter: *[30 days]*
AC-2 (2); Account Management: The information system automatically terminates temporary and emergency accounts after *[Assignment: organization-defined time period for each type of account]*.	AC-2 (2) Parameter: *[24 hours]*
AC-2 (3); Account Management: The information system automatically disables inactive accounts after *[Assignment: organization-defined time period]*.	AC-2 (3) Parameter: *[* • *CSP to limit DoD customer's user accounts to 35 days per DoD policy for access to SaaS* • *CSP to limit DoD SA's admin accounts to 35 days per DoD policy for access to IaaS & PaaS* • *CSP defines the time period for non-user accounts (e.g., accounts associated with CSP infrastructure). The time periods are approved and accepted by the DISA AO]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
AC-6 (1); Least Privilege: The organization explicitly authorizes access to *[Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information]*.	AC-6 (1) Parameter: *[All privileged functions (e.g., System Administrator, Security Administrator, Database Administrator).]* Requirement: The service provider defines the list of security functions. The list of functions is approved and accepted by the DISA AO.
AC-10; Concurrent Session Control: The information system limits the number of concurrent sessions for each system account to *[Assignment: organization-defined number]*.	AC-10 Parameter: *[three (3) sessions for privileged access and two (2) sessions for non-privileged access]* OR *[one session] (more stringent per FedRAMP)*
AC-11; The information system: a. Prevents further access to the system by initiating a session lock after *[Assignment: organization-defined time period]* of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. (Applies to privileged access.)	AC-11 a. Parameter: *[15 minutes, except to fulfill documented, DISA AO approved and validated mission requirement]*
AC-16; Security Attributes: The information system supports and maintains the binding of *[Assignment: organization-defined security attributes]* to information in storage, in process, and in transmission.	AC-16 Parameter: *[If the capability is available, attribute markings should include items such as classification, compartments, and handling instructions, for classified and CUI data]* Requirement: If the service provider offers the capability of defining security attributes, then the security attributes need to be approved and accepted by the DISA AO.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
AC-17 (7); Remote Access: The organization ensures that remote sessions for accessing *[Assignment: organization-defined list of security functions and security-relevant information]* employ *[Assignment: organization-defined additional security measures]* and are audited.	AC-17 (7) Parameter 1: *[security functions and security relevant configuration settings]* Parameter 2: *[session encryption (e.g., SSH or encrypted VPN) and session transcripts]* Guidance: Security functions include but are not limited to: establishing system accounts; configuring access authorizations; performing system administration functions; and auditing system events or accessing event logs. Requirement: The service provider defines the list of security functions and security relevant information available. Security functions and the implementation of such functions are approved and accepted by the DISA AO.
AC-17 (8); Remote Access: The organization disables *[Assignment: organization-defined networking protocols within the information system deemed to be non-secure]* except for explicitly identified components in support of specific operational requirements.	AC-17 (8) Parameter: *[networking protocols within the information system deemed to be non-secure IAW DoDI 8551.1 PPSM Vulnerability assessments including but not limited to: tftp, (trivial ftp); X-Windows, Sun Open Windows; FTP; TELNET; IPX/SPX; NETBIOS; Bluetooth; RPC-services, like NIS or NFS; rlogin, rsh, rexec; SMTP (Simple Mail Transfer Protocol); RIP (Routing Information Protocol); DNS (Domain Name Services); UUCP (Unix-Unix Copy Protocol); NNTP (Network News Transfer Protocol); NTP (Network Time Protocol); Peer-to-Peer]* Requirement: Networking protocols implemented by the service provider are approved and accepted by DISA AO. Guidance: Exceptions to restricted networking protocols are granted for explicitly identified information system components in support of specific operational requirements.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
AC-18 (2); Wireless Access: The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points *[Assignment: organization-defined frequency]*, and takes appropriate action if an unauthorized connection is discovered.	AC-18 (2) Parameter: *[continuously]*
AC-19; Access Control for Mobile Devices: The organization: … g. Applies *[Assignment: organization-defined inspection and preventative measures]* to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	AC-19 g. Parameter: *[physical / logical inspection, and remediation measures (before connection to the network]* NOTE: Mobile devices in this case include but are not limited to Laptops, tablets, and smart phones. Inspection and remediation must occur before connection to the network. Requirement: The service provider defines inspection and preventative measures. The measures are approved and accepted by DISA AO.
AC-22; Publicly Accessible Content: The organization: … d. Reviews the content on the publicly-accessible information for non-public information *[Assignment: organization-defined frequency]*; and ….	AC-22 d. Parameter: *[at least quarterly or as new information is posted]*
Awareness and Training Controls	
AT-3; Security Training: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) *[Assignment: organization-defined frequency]* thereafter.	AT-3 Parameter*: [at least annually]*
AT-4; Security Training Records: The organization: … b. Retains individual training records for *[Assignment: organization-defined time period]*.	AT-4 b. Parameter: For Levels 1-2: *[At least three years]* For Levels 3-6: *[Five years or 5 years after completion of a specific training program]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
Audit and Accountability Controls	
AU-2 (3); Auditable Events The organization reviews and updates the list of auditable events *[Assignment: organization-defined frequency]*.	AU-2 (3) Parameter: *[annually or whenever there is a change in the threat environment]* *NOTE: changes in the threat environment may be detected by the CSP and communicated to the ECSB and/or customer's CNDSP or are communicated to the service provider by the ECSB and/or customer's CNDSP in conjunction with USCYBERCOM.*
AU-3 (1); Content of Audit Records The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject.	AU-3 (1) 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 and, if known, the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, and the purpose for accessing the government data]* Requirement: The CSP will log all access to the government data. The log will contain, if known the name of the individual, the account name, their role, the time they began accessing the government data, the time they concluded accessing the government data, and the purpose for accessing the government data.
AU-6; Audit Review, Analysis, and Reporting: The organization: a. Reviews and analyzes information system audit records *[Assignment: organization-defined frequency]* for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and …	AU-6 a. Parameter: *[every seven days or more frequently if required by an alarm event or anomaly.]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
AU-10 (5); Non-repudiation: The organization employs *[Selection: FIPS-validated; NSA-approved]* cryptography to implement digital signatures.	AU-10 (5) Selection Parameter: *[FIPS-Validated or NSA-approved cryptography as required by the classification level of the information system]* Requirement: The service provider minimally implements FIPS-140-2 validated cryptography (e.g., DOD PKI Class 3 or 4 tokens) for service offerings that include Software-as-a-Service (SaaS) with unclassified email and other applications requiring digital signatures. Requirement: The service provider implements FIPS-140-2 validated or NSA approved cryptography for service offerings that include Software-as-a-Service (SaaS) with email and applications (other than email) requiring digital signatures. The type of cryptography is dependent on the classification of the data and the hosting environment.
AU-11; Audit Record Retention: The organization retains audit records for *[Assignment: organization-defined time period]* to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	AU-11 Parameter: *[…a minimum of 5 years for Sensitive Compartmented Information and Sources And Methods Intelligence information; …a minimum of 1 year for all other information (Unclassified through Collateral Top Secret)]*
AU-12; Audit Generation: The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at *[Assignment: organization-defined information system components]*; …	AU-12 a. Parameter: *[all information system and network components where audit capability is deployed/available]*
Security Assessment and Authorization Controls	

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CA-5; Plan of Action and Milestones: The organization: b. Updates existing plan of action and milestones *[Assignment: organization-defined frequency]*, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	CA-5 b. Parameter: *[at least quarterly or more frequently as required upon an event or anomaly]*
CA-6; Security Authorization: The organization: … c. Updates the security authorization *[Assignment: organization-defined frequency]*	CA-6 c. Parameter: *[at least every three years, or whenever there is a significant change to the system, or whenever there is a change to the environment in which the system operates, or when significant security breaches occur]* 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 require a reauthorization of the information system. The types of changes are approved and accepted by the DISA AO.
CA-7 (2); Continuous Monitoring: The organization plans, schedules, and conducts assessments *[Assignment: organization-defined frequency]*, *[Selection: announced; unannounced]*, *[Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security assessment]]* to ensure compliance with all vulnerability mitigation procedures.	CA-7 (2) Parameter 1: *[annually]* Selection Parameter: *[unannounced]* Selection Parameter: *[penetration testing]* Parameter 2: *[in-depth monitoring PLUS monthly announced scans]*
Configuration Management Controls	

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CM-2 (1); Baseline Configuration: The organization reviews and updates the baseline configuration of the information system: a. *[Assignment: organization-defined frequency]*; b. When required due to *[Assignment organization-defined circumstances]*; and …	CM-2 (1) a. Parameter: *[at least annually]* CM-2 (1) b. Parameter: *[significant system or security relevant changes or security incidents/attacks occur, or upon receipt of USCYBERCOM tactical orders/ directives]* 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 require a review and update of the baseline configuration. The types of changes are approved and accepted by the DISA AO.
CM-2 (5); Baseline Configuration: The organization: a. Develops and maintains *[Assignment: organization-defined list of software programs authorized to execute on the information system]*; …	CM-2 (5) a. Parameter: *[See requirement]* Requirement: The service provider defines and maintains a list of software programs authorized to execute on the information system. The list of authorized programs is approved and accepted by the DISA AO.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CM-3 f.; Configuration Change Control The organization: Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].	CM-3 f. Parameter 1: *[The service provider defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the DISA AO.]* Guidance: DoD uses the term Configuration Control Board (CCB) Alternate terms are acceptable. DoD parameter 2: [*See requirement.*] 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 DoD and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the DISA AO.
CM-5 (5); Access Restrictions for Change: The organization: … b. Reviews and reevaluates information system developer/integrator privileges *[Assignment: organization-defined frequency]*.	CM-5 (5) b. Parameter: *[monthly]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CM-6; Configuration Settings: The organization: a. Establishes and documents mandatory 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; …	CM-6 a. Parameter: *[DoD security configuration and/or implementation guidance (e.g. DoD STIGs, NSA configuration guides, CTOs, DTMs etc.)]* 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). Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc. Information on DoD STIGs and SCAP Benchmarks may be found at http://iase.disa.mil/stigs/index.html Information on NSA configuration guides may be found at http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml Requirements derived from CTOs and DTMs will be provided via the customer's CNDSP

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CM-7; Least Functionality: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: *[Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services]*.	CM-7 Parameter: *[United States Government Configuration Baseline (USGCB) and/or the DoDI 8551.1 PPSM VAs and CAL]* Requirement: The service provider shall use the DoDI 8551.1 PPSM VAs and CAL along with the Center for Internet Security guidelines (Impact 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. The list of prohibited or restricted functions, ports, protocols, and/or services are approved and accepted by the DISA AO. Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc. Information on the DoDI 8551.1 PPSM VAs and CAL may be obtained from the ECSB as DoD CAC/PKI is required for access to http://iase.disa.mil/ports/index.html
CM-7 (1); Least Functionality: The organization reviews the information system *[Assignment: organization-defined frequency]*, to identify and eliminate unnecessary functions, ports, protocols, and/or services.	CM-7 (1) Parameter: *[every 30 days]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CM-8; Information System Component Inventory: The organization develops, documents, and maintains an inventory of information system components that: … d. Includes *[Assignment: organization-defined information deemed necessary to achieve effective property accountability]*; and …	CM-8 d. Parameter: *[See requirement and guidance]* Requirement: The service provider defines information deemed necessary to achieve effective property accountability. Property accountability information are approved and accepted by the DISA AO. Guidance: Information deemed necessary to achieve effective property accountability may include 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 and network address.
Contingency Planning Controls	
CP-2; Contingency Plan: The organization: … b. Distributes copies of the contingency plan to *[Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements]*; … d. Reviews the contingency plan for the information system *[Assignment: organization-defined frequency]*; … f. Communicates contingency plan changes to *[Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements]*.	CP-2 b. Parameter: *[key personnel and organizational elements identified in the contingency plan]* d. Parameter: *[at least annually]* f. Parameter: *[key personnel and organizational elements identified in the contingency plan]* Requirement: The service provider defines a list of key contingency personnel (identified by name and/or by role) and organizational elements. The contingency list includes designated DoD personnel. The list is approved and accepted by the ECSB and customer.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CP-3; Contingency Training: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training *[Assignment: organization-defined frequency]*.	CP-3 Parameter: *[at least annually as defined in the contingency plan]*
CP-4; Contingency Plan Testing and Exercises: The organization: a. Tests and/or exercises the contingency plan for the information system *[Assignment: organization-defined frequency]* using *[Assignment: organization-defined tests and/or exercises]* to determine the plan's effectiveness and the organization's readiness to execute the plan; and …	CP-4 a. Parameter 1: *[at least annually for moderate impact systems; at least every three years for low impact systems]* Parameter 2: *[functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems]* Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to DoD prior to initiating testing. Test plans are approved and accepted by the DISA AO.
CP-7; Alternate Processing Site: The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within *[Assignment: organization-defined time period consistent with recovery time objectives]* when the primary processing capabilities are unavailable; …	CP-7 a. Parameter: *[See requirement]* Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the DISA AO. DoD preferred parameter: *[12 hours (Availability Moderate) OR 1 hour (Availability High) as defined in the contingency plan]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CP-8; Telecommunications Services: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within *[Assignment: organization-defined time period]* when the primary telecommunications capabilities are unavailable.	CP-8. Parameter: *[See requirement]* Requirement: The service provider defines a time period consistent with the business impact analysis. The time period is approved and accepted by the DISA AO. DoD preferred parameter: *[12 hours (Availability Moderate) OR 1 hour (Availability High) as defined in the contingency plan]*
CP-9 ; Information System Backup: The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];	CP-9 a. Parameter: *[daily incremental; weekly full]* 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. The backup storage capability is approved and accepted by the DISA AO. CP-9 b. Parameter: *[daily incremental; weekly full]* 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. The backup storage capability is approved and accepted by the DISA AO. CP-9 c. Parameter: *[daily incremental; weekly full]* 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. The backup storage capability is approved and accepted by the DISA AO.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
CP-9 (1); Information System Backup: The organization tests backup information *[Assignment: organization-defined frequency]* to verify media reliability and information integrity.	CP-9 (1) Parameter: *[not less than monthly, or as defined in the contingency plan]*
Identification and Authentication Controls	
IA-2 (8): Identification and Authentication (Organizational Users): The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.	IA-2 (8) Parameter: *[See requirement]* Requirement: The service provider defines replay-resistant authentication mechanisms. The mechanisms are approved and accepted by the DISA AO.
IA-3; Device Identification and Authentication: The information system uniquely identifies and authenticates *[Assignment: organization-defined list of specific and/or types of devices]* before establishing a connection.	IA-3 Parameter: *[See requirement]* Requirement: The service provider defines a list a specific devices and/or types of devices. The list of devices and/or device types is approved and accepted by the DISA AO. The list should include: All network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).
IA-4; Identifier Management: The organization manages information system identifiers for users and devices by: … d. Preventing reuse of user or device identifiers for *[Assignment: organization-defined time period]*; and e. Disabling the user identifier after *[Assignment: organization-defined time period of inactivity]*.	IA-4 d. Parameter: *[at least 1 year for user identifiers (DoD is not going to specify value for device identifier)]* e. Parameter: *[ninety days for user identifiers]* Requirement: The service provider defines time period of inactivity for device identifiers. The time period is approved and accepted by the DISA AO.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
IA-5; Authenticator Management: The organization manages information system authenticators for users and devices by: … g. Changing/refreshing authenticators *[Assignment: organization-defined time period by authenticator type]*	IA-5 g. Parameter: *[sixty days for passwords; 3 years for CAC/PKI certificate; 3 years for biometrics if applicable.]*
IA-5 (3); Authenticator Management: The organization requires that the registration process to receive *[Assignment: organization-defined types of and/or specific authenticators]* be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	IA-5 (3) Parameter: *[specific authenticators such as but not limited to HSPD12/CAC/ALT PKI smartcard tokens, ECA PKI certificates or tokens (smartcard or USB), onetime password tokens]*
Incident Response Controls	
IR-1; The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]	IR-1 Parameter:*[See guidance]* Guidance: See Section 5.2.4 for details.
IR-3; Incident Response Testing and Exercises: The organization tests and/or exercises the incident response capability for the information system *[Assignment: organization-defined frequency]* using *[Assignment: organization-defined tests and/or exercises]* to determine the incident response effectiveness and documents the results.	IR-3 Parameter 1*: [annually for low/med availability systems; minimally every six months for high availability systems]* Parameter 2: *[See requirement]* Requirement: The service provider provides test plans to DoD annually. Test plans are approved and accepted by the DISA AO prior to test commencing.
IR-6; Incident Reporting: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within *[Assignment: organization-defined time-period]*; and …	IR-6 a. Parameter: For Level 1: *[US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]* For Levels 2-6: *[The timeframes specified by CJCSM 6510.01A (Table C-A-1) and IAW DoDI O-8530.2, unless the data owner provides more restrictive guidance]*

Short Control Verbiage Highlighting the Variable/Parameter	DoD Control Parameter Requirements (Values/Selections)
IR-8; Incident Response Plan: The organization: b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	IR-8 b. Parameter: *[See requirement]* Requirement: 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 ECSB personnel. IR-8 e. Parameter: *[See requirement]* Requirement: 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 ECSB personnel.
Maintenance Controls	
MA-6; Timely Maintenance: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.	MA-6 Parameter 1: *[See requirement]* Requirement: The service provider defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the DISA AO. Parameter 2: *[See requirement]* Requirement: The service provider defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the DISA AO.
Media Protection Controls	

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
MP-2; Media Access: The organization restricts access to *[Assignment: organization-defined types of digital and non-digital media]* to *[Assignment: organization-defined list of authorized individuals]* using *[Assignment: organization-defined security measures]*.	MP-2 Parameter 1: *[See requirement]* Requirement: The service provider defines types of digital and non-digital media. The media types are approved and accepted by the DISA AO. Parameter 2: *[See requirement]* Requirement: The service provider defines a list of individuals with authorized access to defined media types. The list of authorized individuals is approved and accepted by the DISA AO. Parameter3: *[See requirement]* Requirement: The service provider defines the types of security measures to be used in protecting defined media types. The security measures are approved and accepted by the DISA AO.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
MP-5; Media Transport: The organization: a. Protects and controls *[Assignment: organization-defined types of digital and non-digital media]* during transport outside of controlled areas using *[Assignment: organization-defined security measures]*; …	MP-5 a. Parameter 1: Optional for Level 1: *[all digital and non-digital media containing sensitive, controlled, and/or classified information. (e.g., printouts, magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, digital video disks, and other forms of digital or non-digital media as are developed in the future]* Parameter 2: Optional for Level 1 / Required for Levels 2-5: *[FIPS 140-2 validated encryption]* Required for Level 6:*[FIPS 140-2 validated encryption or NSA approved encryption IAW DoDI 5200.1R and other DoD defined security measures]* Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the DISA AO.
Physical and Environmental Protection Controls	
PE-2; Physical Access Authorizations: The organization: … c. Reviews and approves the access list and authorization credentials *[Assignment: organization-defined frequency]*, removing from the access list, personnel no longer requiring access.	PE-2 c. Parameter: *[monthly]*
PE-3; Physical Access Control: The organization: … f. Inventories physical access devices *[Assignment: organization-defined frequency]*; and g. Changes combinations and keys *[Assignment: organization-defined frequency]* and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	PE-3 f. Parameter: *[at least bi-annually]* PE-3 g. Parameter: *[at least annually and as required by security relevant events]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
PE-6; Monitoring Physical Access: The organization: … b. Reviews physical access logs *[Assignment: organization-defined frequency]*; …	PE-6 b. Parameter: *[monthly]*
PE-10; Emergency Shutoff: The organization: … 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 …	PE-10 b. Parameter: *[See requirement]* Requirement: The service provider defines emergency shutoff switch locations. The locations are approved and accepted by the DISA AO.
PE-17; Alternate Work Site: The organization: a. employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites;	PE-17 a. Parameter: *[See requirement]* Requirement: The service provider defines management, operational, and technical information system security controls for alternate work sites. The security controls are approved and accepted by the DISA AO.
Personnel Security Controls	
PS-2; Position Categorization: The organization: … c. Reviews and revises position risk designations *[Assignment: organization-defined frequency]*.	PS-2 Parameter: *[at least annually]*
PS-5; Personnel Transfer: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates *[Assignment: organization-defined transfer or reassignment actions]* within *[Assignment: organization-defined time period following the formal transfer action*].	PS-5 Parameter 1: *[actions to ensure all system accesses no longer required are removed]* Parameter 2: *[24 hours]* Requirement: The service provider defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the DISA AO.
System and Services Acquisition Controls	

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
SA-9 (1); External Information System Services: The organization: … b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by *[Assignment: organization-defined senior organizational official]*.	SA-9 (1) b. Parameter: *[DISA AO]* Requirement: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. Future, planned outsourced services are approved and accepted by the DISA AO.
SA-12; Supply Chain Protection: The organization protects against supply chain threats by employing: *[Assignment: organization-defined list of measures to protect against supply chain threats]* as part of a comprehensive, defense-in-breadth information security strategy.	SA-12 Parameter: *[See requirement]* Requirement: The service provider defines a list of measures to protect against supply chain threats. The list of protective measures is approved and accepted by DISA AO.
System and Communications Protection Controls	
SC-5; Denial of Service Protection: The information system protects against or limits the effects of the following types of denial of service attacks: *[Assignment: organization-defined list of types of denial of service attacks or reference to source for current list]*.	SC-5 Parameter: *[See requirement and note]* Requirement: The service provider defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list is approved and accepted by DISA AO NOTE: The list of denial of service attacks also includes but is not limited to: - consumption of scarce, limited, or non-renewable resources - destruction or alteration of configuration information - physical destruction or alteration of network components
SC-7 (4); Boundary Protection: The organization: … (e) Reviews exceptions to the traffic flow policy *[Assignment: organization-defined frequency]*	SC-7 (4) e. Parameter: *[monthly]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
SC-7 (8); Boundary Protection: The information system routes *[Assignment: organization-defined internal communications traffic]* to *[Assignment: organization-defined external networks]* through authenticated proxy servers within the managed interfaces of boundary protection devices.	SC-7 (8) Parameter 1: *[See requirements]* Parameter 2: *[See requirements]* Requirements: The service provider defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by DISA AO.
SC-10; Network Disconnect: The information system terminates the network connection associated with a communications session at the end of the session or after *[Assignment: organization-defined time period]* of inactivity.	SC-10 For Level 1: Parameter: *[thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users]* For Level 2-6: Parameter: *[10 minutes in band management, 15 minutes for user sessions, except to fulfill documented and validated mission requirements]* Guidance: Long running batch jobs and other operations are not subject to this time limit.
SC-11; Trusted Path: The information system establishes a trusted communications path between the user and the following security functions of the system: *[Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication]*.	SC-11 Parameter: *[See requirement]* Requirement: The service provider defines the security functions that require a trusted path, including but not limited to system authentication, re-authentication, and provisioning or de-provisioning of services (i.e. allocating additional bandwidth to a cloud user). The list of security functions requiring a trusted path is approved and accepted by DISA AO.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
SC-12 (2); Cryptographic Key Establishment and Management: The organization produces, controls, and distributes symmetric cryptographic keys using *[Selection: NIST-approved, NSA-approved]* key management technology and processes.	SC-12 (2) For Levels 2 - 5 Parameter: *[NIST FIPS-Validated Unclassified systems]* For Level 6 Parameter: *[NSA Approved/FIPS-Validated for Classified systems]*
SC-17; Public Key Infrastructure Certificates: The organization issues public key certificates under an *[Assignment: organization-defined certificate policy]* or obtains public key certificates under an appropriate certificate policy from an approved service provider.	SC-17 Parameter: *[See requirement]* Requirement: The service provider defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the DISA AO.
System and Information Integrity Controls	
SI-2 (2); Flaw Remediation: The organization employs automated mechanisms *[Assignment: organization-defined frequency]* to determine the state of information system components with regard to flaw remediation.	SI-2 (2) Parameter: *[Continuously for endpoints; 30 days for internal network scans; Annually for external scans]*
SI-3; Malicious Code Protection: The organization: … c. Configures malicious code protection mechanisms to: - perform periodic scans of the information system *[Assignment: organization-defined frequency]* and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator*; *[Assignment: organization-defined action]*] in response to malicious code detection;	SI-3 c. Parameter 1: *[at least weekly]* Parameter 2 : *[block malicious code; quarantine malicious code; send alert to administrator]* Parameter 3 : *[send alert to USCYBERCOM via DoD customer's CNDSP, and send alert to ECSB]*

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
SI-4; Information System Monitoring The organization: a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks;	SI-4 a. Parameter: *[See requirement]* Requirement: CSP defines monitoring objectives and processes which ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise. The monitoring objectives and processes are approved and accepted by the DISA AO. NOTE: DoD Sensor placement and monitoring requirements are found in CJCSI 6510.01F

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
SI-4 (5); Information System Monitoring: The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: *[Assignment: organization-defined list of compromise indicators]*.	SI-4 (5) Parameter: *[protected information system files or directories are modified without notification by appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality is disabled or modified reducing audit visibility; audit or log records are deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running outside of baseline system profile; utilities, tools, or scripts are saved or installed on production systems without clear indication of their use or purpose]* Requirement: The service provider defines additional compromise indicators as needed. Guidance: Alerts may be generated from a variety of sources including but not limited to malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

Short Control Verbiage Highlighting the Variable/Parameter	**DoD Control Parameter Requirements (Values/Selections)**
SI-5; Security Alerts, Advisories, and Directives The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and	SI-5 a. Requirement: The "designated external organization" is defined as CND Tier II. CSPs must be able to receive and act upon warnings and notifications that are sent by CND Tier II. These notifications may be generated by Tier I or II CND and will include guidance for or countermeasures to be taken by CSPs. Guidance: The CSP should describe how they plan to act upon warnings and notification from DoD CND Tier II. SI-5 c. Parameter: [*All staff with system administration, monitoring, and/or security responsibilities including but not limited to DOD CND Tier II*] Requirement: The service provider defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated DoD CND Tier II personnel.
SI-6; Security Functionality Verification: The information system verifies the correct operation of security functions [Selection (one or more): *[Assignment: organization-defined system transitional states]*; upon command by user with appropriate privilege; periodically every *[Assignment: organization-defined time-period]*] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; *[Assignment: organization-defined alternative action(s)]*] when anomalies are discovered.	SI-6 Parameter 1: *[upon system startup and/or restart, upon command by user with appropriate privileges, and periodically every]* Parameter 2 : *[monthly]* Parameter 3 : *[notifies system administrator]*

Appendix N Recommended DoD Availability Controls for Contract Consideration

DoD customers of a cloud service provider must review this list of control enhancements to determine which are needed for their cloud service use-case. Subsequently they must ensure the necessary control enhancements are included in their Service Contract or SLA with the cloud provider. Some negotiation may be required for their inclusion and the level of service required to meet them.

Table 53 indicates which ECSB Impact Levels each control enhancement is applicable to or negotiable for. Availability-related control parameter values are added to applicable Impact Levels. The reduced number of control enhancements at the higher levels is due to those controls already being required and non-negotiable for inclusion at that level.

If the DoD cloud customer elects to invoke any of these controls, the DoD customer and CSP must ensure control parameters are defined in the service contract or a Service Level Agreement (SLA). The values presented in the table reflect the values that DoD typically would use. These are intended to be recommendations toward achieving the negotiated value.

Table 53 – DoD Recommended Availability Controls for Contract Consideration

Added Control	Description	L1	L2	L3	L4	L5	L6
AU-5 (1)	The information system provides a warning when allocated audit record storage volume reaches *[Assignment: organization-defined percentage]* of maximum audit record storage capacity.	*[a maximum of 75 percent OR as negotiated in the SLA]*					
AU-5 (2)	The information system provides a real-time alert when the following audit failure events occur: *[Assignment: organization-defined audit failure events requiring real-time alerts]*.	*[auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded OR as negotiated in the SLA]*					

Added Control	**Description**	**L1**	**L2**	**L3**	**L4**	**L5**	**L6**
CM-3 (1)	The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify designated approval authorities; (c) Highlight approvals that have not been received by *[Assignment: organization-defined time period]*; (d) Inhibit change until designated approvals are received; and (e) Document completed changes to the information system.					*[7 days or as negotiated in the SLA]* *NOTE: This control is a requirement for L5 & L6, however the value of part c may be negotiated*	
CP-2 (1)	The organization coordinates contingency plan development with organizational elements responsible for related plans.	**X**					
CP-2 (2)	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	**X**					
CP-2 (3)	The organization plans for the resumption of essential missions and business functions within *[Assignment: organization-defined time period]* of contingency plan activation.	*[12 hours (Availability Moderate); 1 hour (Availability High)]*					
CP-2 (4)	The organization plans for the full resumption of missions and business functions within *[Assignment: organization-defined time period]* of contingency plan activation.	*[12 hours (Availability Moderate); 1 hour (Availability High)]*					

Added Control	Description	L1	L2	L3	L4	L5	L6
CP-2 (5)	The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	**X**	**X**	**X**	**X**	**X**	**X**
CP-2 (6)	The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.	**X**	**X**	**X**	**X**	**X**	**X**
CP-3 (1)	The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	**X**	**X**	**X**	**X**	**X**	**X**
CP-4 (2)	The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.	**X**	**X**	**X**	**X**	**X**	**X**
CP-6 (2)	The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	**X**	**X**	**X**	**X**	**X**	**X**
CP-7 (4)	The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.	**X**	**X**	**X**	**X**	**X**	**X**

Added Control	Description	L1	L2	L3	L4	L5	L6
CP-8 (3)	The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.	**X**	**X**	**X**	**X**	**X**	**X**
CP-8 (4)	The organization requires primary and alternate telecommunications service providers to have contingency plans.	**X**	**X**	**X**	**X**	**X**	**X**
CP-9 (2)	The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	**X**	**X**	**X**	**X**	**X**	**X**
CP-9 (3)	The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.	**X**					
CP-9 (5)	The organization transfers information system backup information to the alternate storage site *[Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]*.	*[Continuously (Availability High);24 hours (Availability Moderate);7 days (Availability Low)]*					
IR-5 (1)	The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	**X**	**X**	**X**	**X**	**X**	**X**

Added Control	**Description**	**L1**	**L2**	**L3**	**L4**	**L5**	**L6**
MA-2 (2)	The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.	**X**	**X**	**X**	**X**	**X**	**X**
PE-9 (2)	The organization employs automatic voltage controls for *[Assignment: organization-defined list of critical information system components]*.	*[all IT Components Critical to Execution of Missions OR as negotiated in the SLA]*					
PE-11 (1)	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	**X**	**X**	**X**	**X**	**X**	**X**
PE-11 (2)	The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.	**X**	**X**	**X**	**X**	**X**	**X**
PE-12 (1)	The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.	**X**	**X**	**X**	**X**	**X**	**X**
PE-13 (4)	The organization ensures that the facility undergoes *[Assignment: organization-defined frequency]* fire marshal inspections and promptly resolves identified deficiencies.	*[Annual or as negotiated in the SLA]*					
PE-14 (1)	The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.	**X**	**X**	**X**	**X**	**X**	**X**

Added Control	**Description**	**L1**	**L2**	**L3**	**L4**	**L5**	**L6**
PE-14 (2)	The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.	**X**	**X**	**X**	**X**	**X**	**X**
SC-5 (1)	The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.	**X**	**X**	**X**	**X**	**X**	**X**
SC-5 (2)	The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	**X**	**X**	**X**	**X**	**X**	**X**
SC-6	The information system limits the use of resources by priority.	**X**					
SC-12 (1)	The organization maintains availability of information in the event of the loss of cryptographic keys by users.	**X**	**X**	**X**	**X**	**X**	**X**
SI-13	The organization: a. Protects the information system from harm by considering mean time to failure for *[Assignment: organization-defined list of information system components]* in specific environments of operation;	*[all IT Components Critical to Execution of Missions OR Any component within a system requiring high availability OR as negotiated in the SLA]*					