Critical Review/Technology Assessment (CR/TA)
November 2014

Cloud Computing for the Government Sector

Cyber Security and Information Systems Information Analysis Center (CSIAC)
Assured Information Security (AIS)

Joint endeavor by CSIAC and AIS

Cloud Computing for the Government Sector

Critical Review/Technology Assessment (CR/TA)
November 2014

Table of Contents

Section

List of Figures

List of Tables

1 Summary

Department of Defense (DoD) organizations often process sensitive data that cannot be entrusted to 3rd party organizations without precautions and protections. The Defense Information Systems Agency (DISA) is in the process of defining these protections and the process that ensures their implementation. Our research explores the gap between the existing state of cloud computing and DoD cloud provider requirements by consolidating the DISA draft requirements, which draw from some dozen other documents and government standards. The resulting requirements can be compared to existing, major cloud providers, also defined in this research, to understand the feasibility of compliance with DISA standards. We recommend further research to determine the feasibility of adapting to these requirements, particularly for major providers, as well as for the organizations using cloud computing.

1.1 Audience

This report's intended audience includes cloud providers interested in providing service to DoD organizations, the DoD organizations that intend to use cloud services, the auditing entities that will ensure compliance with DISA requirements, and any vendor or organization interested in supporting the deployment of cloud services within the DoD.

2 Cloud Provider Analysis

2.1 The Four Cloud Models

There are three traditional cloud computing service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [3]. More recently a fourth model has emerged, Network as a Service (NaaS) [4]. Table 2 describes each service and the features each typically offers.

Table 1: Each progressing type of cloud environment builds upon the foundations of earlier models.

Cloud Model	Typical Offerings									
	Network Infrastructure	Virtual Machines	Servers	Storage	Load Balancing	Operating System	Execution Environment	Database	Web Server	Applications
Network as a Service (NaaS)	✓									
Infrastructure as a Service (IaaS)	✓	✓	✓	✓	✓					
Platform as a Service (PaaS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Software as a Service (SaaS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

In some instances a cloud service may be classified under two or more models. For example, Amazon Web Services is both an IaaS and PaaS provider [1], giving customers the ability to choose different levels of service.

2.2 Cloud Services

When cloud computing was largely limited to subscriptions with a single provider, the four cloud models sufficiently described the type of service consumers could expect to receive. This is no longer the case as other types of providers have emerged in recent years. Now there are organizations dedicated exclusively to building cloud software for public and private clouds. There are other providers that simply resell services. Still others are dedicated to providing managed services and provide cloud services as part of their approach. Knowing which type of service a provider offers is essential to understanding the type of service you can expect to receive. There are six types of services, defined in the table below, with the four cloud models all falling under the first type, “Cloud Services Provider” [1].

Table 2: Cloud service provider types and self-categorization figures from survey respondents, excerpted from the Talkin’Cloud 2013 annual report on the top 100 cloud service providers [1].

ID	Type	Description	Percentage of Providers Self-Identified as this Type of Provider	
			2011	2012
1	**Cloud Services Provider**	Cloud Service Providers offer a paid service for cloud resources and include the traditional models: • SaaS (software as a service) • IaaS (infrastructure as a service) • PaaS (platform as a service) We also classify the emerging network as a service (NaaS) model under this category.	63.4%	71.0%
2	**Cloud Services Brokerage**	Cloud brokers simply resell cloud services to customers. Brokerages typically offer collections of services and may	34.8%	42.5%

		integrate them for ease of use.		
3	**Cloud Services Aggregator**	Cloud service aggregators provide access to cloud services to allow valued added resellers (VARS) and managed services providers (MSPs) to deploy multiple third-party cloud services for customers.	14.3%	18.8%
4	**Cloud Builder**	Cloud builders implement and deploy clouds for their customers, who will manage them.	33.0%	36%
5	**VAR with Cloud Computing Expertise**	Valued added resellers (VARs) offer on-premises IT projects, but also offer cloud services.	42.0%	29%
6	**MSP with Cloud Computing Expertise**	Managed service providers (MSPs) offer on-premises and cloud based network management services.	58.9%	51.6%

Many cloud services do not fit neatly into a single category. This is evidenced by the percentages for self-identified service types in the table, which exceed 100%. This lack of a clear categorization makes it particularly difficult to assess providers. For example, many cloud builders (e.g., Citrix) actually do not sell a service to cloud consumers; they sell the infrastructure needed to deploy a cloud to the service providers (CSPs). In spite of this, they are often rated as a major cloud provider, as in [2]. Figure 1 describes the relationship between cloud service types.

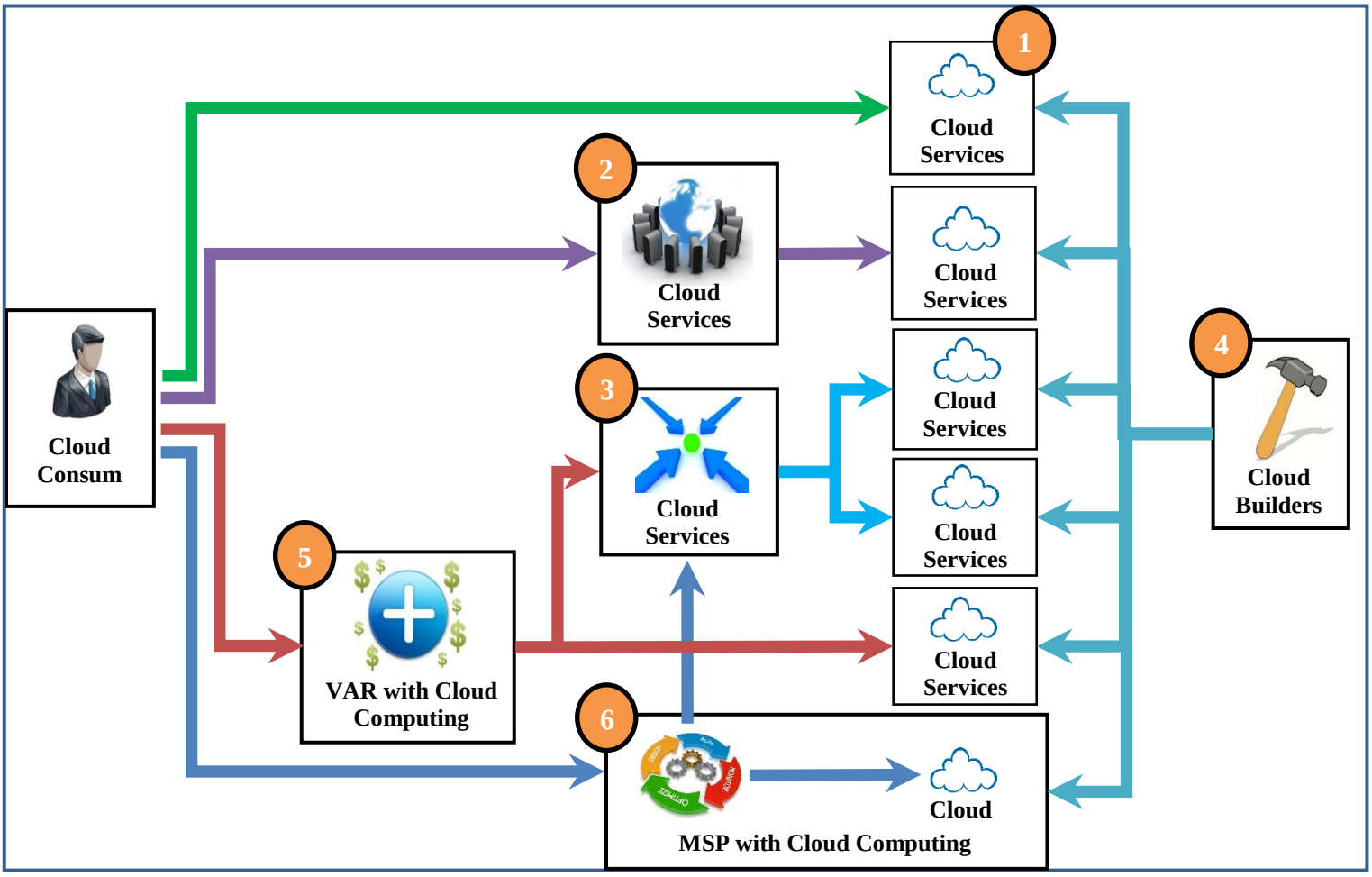


Figure 1: This overview describes the relationship between each type of cloud service and the end consumer.

Any of these services may be relevant to a cloud consumer. For example, if a consumer wishes to deploy a private cloud, they may need to enlist the support of a cloud builder, if the consumer needs a wide variety of services, they may instead turn to a cloud services aggregator. These categories are essential to understanding a provider's service, but many providers span multiple options (e.g., many cloud services providers are also cloud builders). Furthermore, each type of service can be described in terms of the four cloud models. For example, a cloud builder may specialize in IaaS offerings and a cloud services aggregator may focus on SaaS. Finally, organizations often do not define themselves in terms of these classifications. These factors make it challenging to accurately portray a cloud provider's services. This document will work to define providers, both in terms of the four cloud models and the service types.

2.3 Overview of Major Public Cloud Providers

The following cloud providers are potential candidates for use within the DoD. The Talkin'Cloud 2013 annual report on the top 100 cloud service providers conducted a broad survey of cloud consumers to identify which services they used within their organization [1]. While this survey does not include NaaS providers we identified several major providers in this area. Due to the recent emergence of the NaaS model, market share and other information is not readily available. The table below aggregates this information along with key features of each provider.

Table 3: Major Cloud Service Providers drawn from the Talkin'Cloud 2013 survey of cloud consumers [1] and other resources.

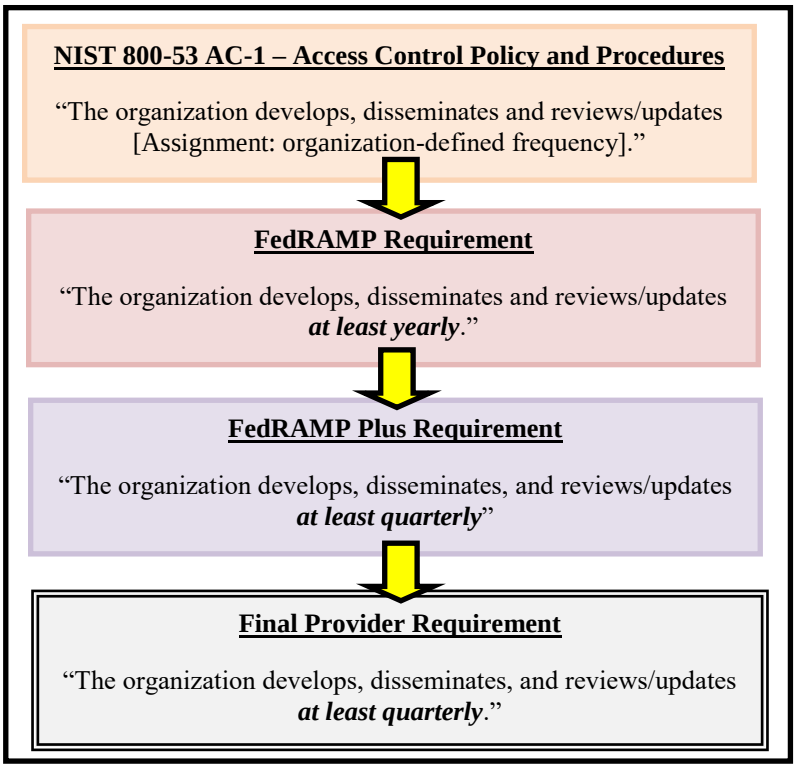
Provider	Cloud Model				Rank (by Model)	Usage [1]	Description and Other Categorizations	License		Billing Model			Support	
	SaaS	*PaaS*	*IaaS*	*NaaS*				*Open*	*Proprietary*	*Pay as you go*	*Subscription*	*Licensed*	*Included*	*Additional*
Citrix Systems (e.g., GoToMeeting) [5] [6]	✓				1	34.9%	Communications, Webinars, Data Sharing and Storage, Email		✓		✓		✓	
Microsoft Office 365 [7]	✓				2	34.8%	MS Office, email, calendars, conferencing, file sharing		✓					
Google Apps [8]	✓				3	30.1%	Communication, Calendars, Google Docs, etc.		✓		✓		✓	
Salesforce.com [9]	✓				4	29.6%	Customer relationship management, Contacts Management, Marketing		✓		✓		✓	
Cisco Systems (e.g., WebEx Meetings) [10] [11]	✓				5	21.0%	Communication, Training, Telepresence, Social Networking, Technical Support		✓		✓		✓	
McAfee [12]	✓				6	19.9%	**Cloud Builder** (Security)**,** Endpoint, email, web, and network security		✓			✓		
DropBox [13]	✓				7	19.8%	Storage, File Sharing		✓		✓		✓	
LogMeIn [14]	✓				8	17.7%	IT Management, Remote Desktop, IT Support, VPN		✓		✓		✓	
Trend Micro [15] [16] [17]	✓				9	14.0%	**Cloud Builder** (Security), Encryption, Whole Volume Encryption, Access Control, Key Management, Auditing, Anti-Virus, Email		✓			✓		
Intermedia [18] [19]	✓				10	13.4%	**Cloud Services Aggregator, Value Added Reseller,** Microsoft Exchange, Lync Secure Chat, Conferencing, Microsoft SharePoint, File Management, Backup & Security		✓		✓		✓	
ConnectWise [20]	✓				11	12.9%	Professional Services Automation, Help Desk and Service Management, Sales, Marketing, and Account Management, Finance Management, Project Management, Procurement and Inventory		✓					
Symantec.cloud [21]	✓				12	12.8%	Email Management, Data Backup, Anti-Virus,		✓			✓		

							Instant Messaging, Email Security							
Amazon Web Services [22] [23]		✓	✓		1,1	48.4%	On-Demand Instances, Reserved Instances, AWS GovCloud, Elastic IP addresses, Elastic Block Store		✓	✓	✓		✓	✓
Microsoft Windows Azure [24] [25] [26]		✓	✓		2,2	29.1%	Infrastructure, Application Development and Testing, Mobile App Development, Hadoop, Web Server, Content Delivery, Storage, Backup, Recover, Identity and Access Management.		✓	✓	✓		✓	✓
Salesforce Force.com [27]		✓			3	11.8%	Application Development Platform, Application Delivery, per app/user subscription		✓		✓			✓
Google App Engine [28]		✓			4	11.3%	Application Development, Datastore API, Search API, Email API, Storage		✓		✓			✓
Rackspace [29] [30]		✓	✓		5,3	10.2%, 14.0%	From 1GB 1vCPU, 20GB SSD, 200Mb/s Bandwidth to 120GB RAM, 32 vCPUs, 40GB SSD, 1,200 GB Disk Storage, 10,000 Mb/s bandwidth		✓	✓	✓		✓	
ThinkGrid [31] [32]		✓			6	4.8%	Self-service and billing, hosted virtual desktop, Virtual Server, Unified Communications, and Hosted Email.		✓	✓			✓	
Red Hat OpenShift (Cloud Foundry) [33][34]		✓			7	3.2%	Development support environment, Java, Ruby, PHP, Phython, and Perl	✓			✓		✓	✓
RightScale [35] [36]		✓			8	2.2%	General PaaS provider		✓	✓	✓		✓	✓
Google Compute Engine [37] [38]			✓		4	9.1%	Designed for large-scale computing workloads on Linux virtual machines		✓	✓				✓
HP Cloud [39] [40]			✓		5	7.0%	Computation, Block Storage, Object Storage, Bandwidth, DNS, Relational Database		✓	✓			✓	
OpenStack [41]			✓		5	6.5%	**Cloud Builder**, Open Source, Does not sell service (offers software for building a private or public cloud), Used by Cloudwatt, DreamCompute, eNocloud, HP, Rackspace, and Ulticloud	✓		-	-	-	✓	
Verizon Terremark [42] [43] [44]			✓		6	6.5%	Base plan consists of one virtual processor, 0.5 GB RAM, System storage is subscription only at $0.25/month per GB and bandwidth is $0.17/GB transferred.		✓	✓	✓		✓	
IBM SmartCloud Enterprise [45] [46] [47] [48]			✓		7	5.9%	IBM SmartCloud Enterprise is an IaaS provider that serves as the basis for IBM SmartCloud Application Services (a PaaS offering)		✓		✓		✓	
SoftLayer CloudLayer [49]			✓		8	5.4%	IBM owned, virtual servers, remote storage, and content delivery network		✓	✓	✓			
CenturyLink Savvis [50] [51] [52]			✓		9	4.8%	Offers Xen and VMware based servers			✓	✓		✓	✓
Artisan Infrastructure [53] [54]			✓		10	3.8%	Wholesale Only, **Cloud Builder/Provider** that sells service to brokers, aggregators, VARs, and MSPs for resale to end users.		✓	✓	✓			
Aryaka Networks [55]				✓	-	-	WAN as a service		✓	-	-	-	-	-
Aerohive Networks [56]				✓	-	-	Pay as you go network infrastructure with 1 year terms of commitment.		✓	✓	✓	-	✓	-
Pertino [57]				✓	-	-	5 plans, basic (free) to enterprise (40+ devices)		✓		✓	-	-	-
OpenNaas [58]				✓	-	-	**Cloud Builder**, Open Source network as a service infrastructure and software.	✓		-	-	-	✓	

3 Certification Process

All providers must undergo certification to provide cloud services to Federal customers. At a minimum every provider of Federal cloud services must attain FedRAMP certification, governed by a Joint Accreditation Board (JAB) [http://www.gsa.gov/portal/category/102439]. Each individual Federal agency may also implement their own certification process and additional requirements, beyond FedRAMP. This is referred to as "*FedRAMP Plus*". Cloud providers must first identify which agency their customer falls under and gather all requirements, both FedRAMP and agency specific.

3.1 Understanding Requirements



Certification requirements rely on a combination of well-defined controls and more abstract procedures and practices. For both FedRAMP and FedRAMP Plus, the controls are derived from the NIST 800-53 control set, which carefully defines the policy and security settings of information systems. The NIST 800-53 control set carefully defines and uniquely identifies each configurable information system requirement, for example, item AC-1 under *Access Control Policy and Procedures* states that *The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]"*. FedRAMP selects a subset of the NIST 800-53 controls, such as AC-1, and provides the relevant parameters required to attain certification, in this case "*at least yearly*". For FedRAMP plus, agencies may define additional requirements, but most often choose to identify a NIST 800-53 requirement and provide a parameter that is stricter than the one found in FedRAMP (e.g., "*at least quarterly*" for AC-1). In almost all cases FedRAMP Plus requirements remain in very early draft form and this research has identified cases where agency parameters to controls were less stringent than FedRAMP parameters. In these cases, whether intentional or due to error, the cloud provider must still meet the more stringent requirement, as FedRAMP certification is a prerequisite to any FedRAMP Plus certification. In all instances, the provider should adhere to the most stringent requirement.

The second set of requirements defines basic policy. For example, FedRAMP certification requires providers to describe, in detail, their incident response policy. In these instances, the provider must provide documentation defining their response process, taking into account the granting authority's guidance. The resulting policies are reviewed and evaluated prior to granting certification. As with the control sets, guidance from both FedRAMP and FedRAMP Plus must be considered to ensure that the resulting policy meets all requirements. This is particularly important, since any revisions to these policies must be reviewed and accepted by all certifying boards.

3.2 Identifying Requirements

The requirements gathering process should begin by identifying the Federal cloud consumers targeted by a cloud capability. Once identified, the appropriate FedRAMP and FedRAMP Plus requirements can be collected. FedRAMP requirements are discussed in detail throughout Section 4 and FedRAMP Plus is described in Section 5. Providers must then merge the requirements for both controls and policy definitions. The merged controls should consist of a list of controls, drawn from the NIST 800-53 set, and a single set of parameters that represent the strictest requirements from either FedRAMP or FedRAMP Plus. Whenever possible, we recommend consolidating these requirements prior to seeking FedRAMP certification, since any changes must be re-evaluated and certified by the FedRAMP Joint Authorization Board (JAB).

4 FedRAMP Certification

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to the authorization, security assessment, and continuous monitoring of cloud products and services [http://cloud.cio.gov/fedramp]. FedRAMP is governed by the Joint Accreditation Board (JAB), which consists of DoD, DHS, and GSA Chief Information Officers (CIOs). There are numerous models of varying complexity used to describe the FedRAMP accreditation process. In addition to requirements imposed on cloud providers, the agencies employing cloud services are also required to fulfill responsibilities, such as reporting cloud services that do not meet FedRAMP requirements and monitoring any security controls designated to the agency [http://www.gsa.gov/portal/content/133675]. As of March 2013, eleven cloud providers have received FedRAMP provisional authority to operate (ATO) and four have received outright ATO. The table below outlines each of these providers.

Table 4: FedRAMP has granted authorization (provisional and final ATO) to fifteen providers.

Provider	Cloud Environment	Type	Provisional ATO	ATO
Akamai	Content Delivery Services	IaaS	✓	
AT&T	Storage as a Service (StaaS)	IaaS	✓	
Autonomic Resources LLC	ARC-P IaaS	IaaS	✓	
CGI Federal	CGI Federal Cloud	IaaS	✓	
Concurrent Technologies Corporation	Unclassified Remote Hosted Desktops (URHD)	SaaS	✓	
Hewlett Packard	HP Enterprise Cloud Services – Virtual Private Cloud (ECS-VPC)	IaaS	✓	
IBM	Smartcloud for Government	IaaS	✓	
Lockheed Martin	Solutions as a Service (Solas) Community Cloud	IaaS	✓	
Microsoft	Cloud Infrastructure	IaaS	✓	
Microsoft	Windows Azure Public Cloud Solution	PaaS	✓	
Oracle Corporation	Federal Managed Cloud Services (FMCS)	PaaS	✓	
AINS, Inc.	eCase SaaS	SaaS		✓
Amazon Web Services	AWS East/West US Public Cloud	IaaS		✓
Amazon Web Services	AWS Government Community Cloud	IaaS		✓
United States Department of Agriculture	USDA National Information Technology Center IaaS	IaaS		✓

The authorization process for is shown in the table below.

Table 5: The FedRAMP authorization process consists of 13 basic steps.

Step	Title	Responsibility	Description
1	Initiate Request	CSP	The cloud service provider can submit an Initiation Request Form to the FedRAMP program office. [http://www.gsa.gov/portal/category/103003].
2b	Submit FIPS 199 Form	CSP	The CSP completes the FIPS 199 form, used to determine the impact level to be supported by the cloud information system/service. The provider categorizes their system based on the data types currently stored and not leveraging agency data [http://www.gsa.gov/portal/category/103003]. No guidance is given as to whether this step should occur before, during, or after step 2b.
2b	Assign Systems Security Officer	FedRAMP PMO	The FedRAMP program office assigns the SSO to support the CSP in implementing security controls, documentation, and the security assessment [http://www.gsa.gov/portal/category/103003].
3	Initiation Request Review	FedRAMP PMO	The FedRAMP PMO assesses and approves the initiation request and the FIPS 199 worksheet.
4	Negotiation	FedRAMP PMO, CSP, Sponsoring Agency	The FedRAMP PMO enters into negotiations with the CSP and any sponsoring agency, if applicable, to define an assessment of the CSP system.
5	CTW and CIS Document Submission	CSP	The CSP must complete the Control Tailoring Workbook (CTW) and the Control Implementation Summary (CIS) and submit these documents to the FedRAMP PMO.

6	CTW and CIS Document Review	FedRAMP PMO	The PMO reviews and rejects documents until they have been verified as complete and compliant.
7	JAB Review	FedRAMP PMO, JAB	The Joint Authorization Board (JAB) reviews documentation. If the JAB identifies any concerns, the FedRAMP PMO informs allows the CSP to address these concerns and resubmit.
8	Document System Security Plan	CSP	The CSP must document and submit the security control implementation in the System Security Plan template along with any supporting documentation to the FedRAMP SSO [http://www.gsa.gov/portal/category/103135].
9	SSO Review of System Security Plan	FedRAMP PMO (SSO)	The FedRAMP SSO reviews the System Security Plan and approves it after the CSP has addressed concerns.
10	JAB Review of System Security Plan	JAB	The JAB reviews the SSP and approves it after concerns have been addressed by the CSP.
11	Security Testing	CSP	The CSP contracts with a FedRAMP accredited 3rd Party Assessment Organization to validate the security control implementation.
12	JAB Reviews Security Assessment Package	JAB	The JAB reviews the security assessment package.
13a	FedRAMP PMO Grants Provisional Authorization	JAB	Based on the outcome of step 12, if approved, the JAB awards provisional authorization to the CSP.
13b	FedRAMP PMO Denies Provisional Authorization	JAB	Based on the outcome of step 12, if declined, provisional authorization is not awarded to the CSP.

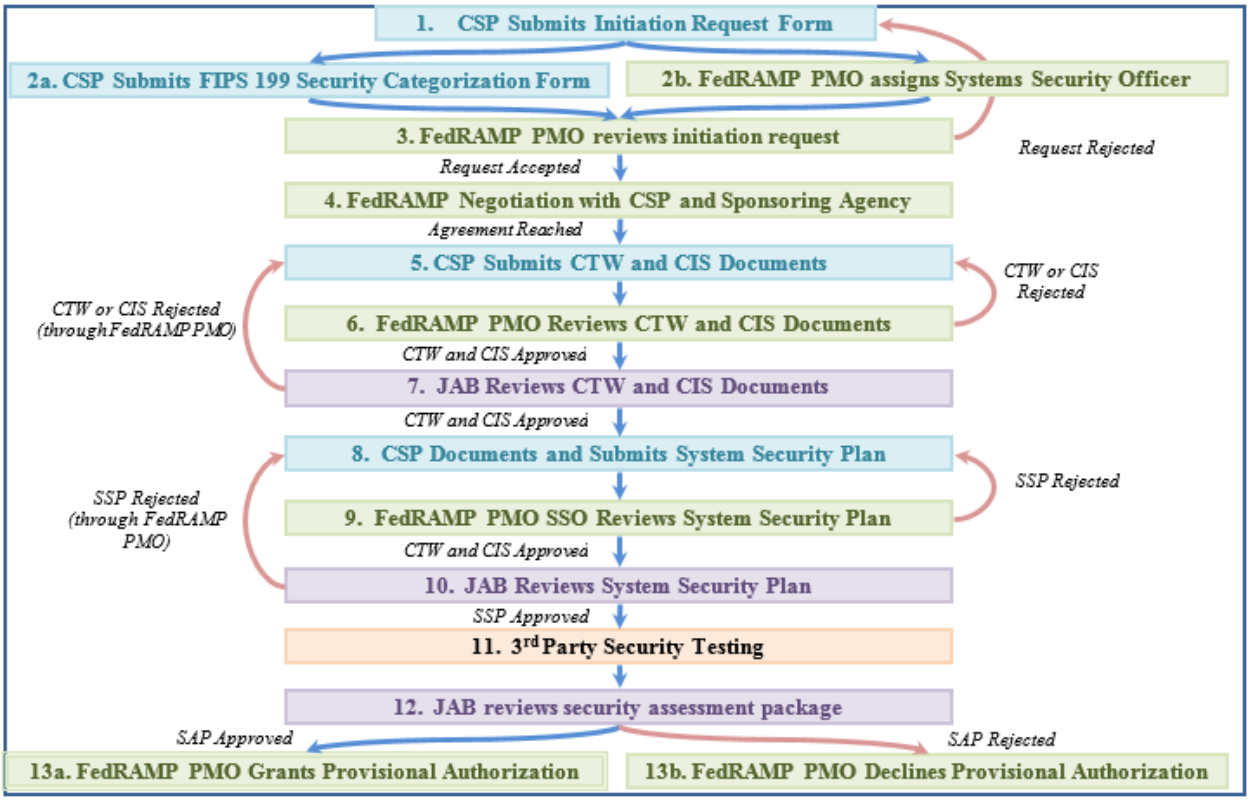


Figure 2: The Cloud Service Provider, FedRAMP PMO, JAB, Supporting Agencies, and 3rd Party Security Testers all take part in the authorization process.

It should be noted that, while step 2b mentions implementation of security controls, no step is defined that assigns this important task. It can be assumed that implementation of security controls must occur prior to the security testing (step 11). The FedRAMP PMO Systems Security Officer (SSO) will review the FIPS 199 form and determine if the CSP is required to meet either FedRAMP low or medium baseline requirements. Section 4.1 combines the NIST 800-53 requirement with FedRAMP low parameters to consolidate each of the FedRAMP low requirements. Section 4.2 does this for FedRAMP medium

requirements. The guidance for ongoing assessment & authorization is found in section 4.3. Together, this information provides a relatively complete depiction of the FedRAMP requirements. Additional information is available in the FedRAMP template files, available at http://www.gsa.gov/portal/content/136423.

4.1 FedRAMP Baseline Controls for Low Certification

The FedRAMP low requirements consist of 116 controls taken from the NIST 800-53 control set [63], with additional parameters defined by FedRAMP [62]. The controls are taken from 16 different control categories, shown in the table below.

Table 6: The 116 FedRAMP controls are organized within 16 control categories.

Category	Category Title
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environment Protections
PS	Personnel Security
PL	Planning Requirements
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity

4.1.1 Access Control Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
AC-1	Access Control Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
AC-2	Account Management	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: • temporary accounts that are no longer required; and • accounts of terminated or transferred users; i. Granting access to the system based on: • a valid access authorization; • intended system usage; and • other attributes as required by the organization or associated missions/business functions j. Reviewing accounts *at least annually*.

AC-3	Access Enforcement	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.
AC-7	Unsuccessful Login Attempts	The information system: a. Enforces a limit of *not more than three* consecutive invalid login attempts by a user during *fifteen minutes*; and b. Automatically *locks the account/node for thirty minutes* when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.
AC-8	System Use Notification	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: • users are accessing a U.S. Government information system; • system usage may be monitored, recorded, and subject to audit; • unauthorized use of the system is prohibited and subject to criminal and civil penalties; and • use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: • Displays the system use information when appropriate, before granting further access; • Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and • Includes in the notice given to public users of the information system, a description of the authorized uses of the system. *The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB.* *The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.* *If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB.*
AC-14	Permitted Actions without Identification or Authentication	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.
AC-17	Remote Access	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system.
AC-18	Wireless Access	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system.
AC-19	Access Control for Mobile Devices	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and

		g. *The service provider defines inspection and preventative measures, which must be approved and accepted by JAB.* The service provider applies these 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-20	Use of External Information Systems	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.
AC-22	Publicly Accessible Content	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information *at least quarterly*; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

4.1.2 Awareness and Training Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
AT-1	Security Awareness and Training Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
AT-2	Security Awareness	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and *at least annually* thereafter.
AT-3	Security Training	The organization provides role-based security-related training: a. before authorizing access to the system or performing assigned duties; b. when required by system changes; and c. *At least every three years* thereafter.
AT-4	Security Training Records	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for *at least three years*.

4.1.3 Audit and Accountability (AU) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
AU-1	Audit and Accountability Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
AU-2	Auditable Events	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: • *Successful and unsuccessful account logon events* • *Account management events* • *Object access* • *Policy change* • *Privilege functions* • *Process tracking, and*

		• *System events* • *For Web applications:* ○ *All administrator activity,* ○ *Authentication checks,* ○ *Authorization checks,* ○ *Data deletions,* ○ *Data access,* ○ *Data changes, and* ○ *Permission changes* b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be *continually* audited within the information system *and receives approval and acceptance by JAB*.
AU-3	Content of Audit Records	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.
AU-4	Audit Storage Capacity	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
AU-5	Response to Audit Processing Failures	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: • *low-impact: overwrite oldest audit records;* • *moderate-impact: shut down*
AU-6	Audit Review, Analysis, and Reporting	The organization: a. Reviews and analyzes information system audit records *at least weekly* for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
AU-8	Time Stamps	The information system uses internal system clocks to generate time stamps for audit records.
AU-9	Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
AU-11	Audit Record Retention	The organization retains audit records for *at least 90 days* to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. *The service provider further preserves audit records off-line for a period that is in accordance with NARA requirements*.
AU-12	Audit Generation	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at *all information system components where audit capability is deployed*; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

4.1.4 Assessment and Authorization (CA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
CA-1	Security Assessment and Authorization Policies and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.
CA-2	Security Assessments	The organization: a. Develops a security assessment plan that describes the scope of the assessment including:

		• Security controls and control enhancements under assessment; • Assessment procedures to be used to determine security control effectiveness; and • Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system *at least annually* to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.
CA-2 (1)	Security Assessments	The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.
CA-3	Information System Connections	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.
CA-5	Plan of Action and Milestones	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones *at least quarterly* based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
CA-6	Security Authorization	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization *at least every three years or when a significant change occurs. A 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 systems. The types of changes are approved and accepted by the JAB.*
CA-7	Continuous Monitoring	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials *monthly*.

4.1.5 Configuration Management (CM) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
CM-1	Configuration Management Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
CM-2	Baseline Configuration	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
CM-4	Security Impact Analysis	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
CM-6	Configuration Settings	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using *United States Government Configuration Baseline (USGCB)* that reflect the most restrictive mode consistent with operational requirements; • *If USGCB is not available, the service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establish its own configuration settings.*

		• *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). Checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc* b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
CM-7	Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the functions, ports, protocols, and/or services *defined in the United States Government Configuration Baseline (USGBC)*. *The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. The list of prohibited or restricted functions, ports, protocols, and/or services are approved and accepted by the JAB.* *Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc*
CM-8	Information System Component Inventory	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes organization-defined information deemed necessary to achieve effective property accountability; and • *The service provider defines information deemed necessary to achieve effective property accountability. Property accountability information are approved and accepted by the JAB.* • *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.* e. Is available for review and audit by designated organizational officials.

4.1.6 Contingency Planning (CP) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
CP-1	Contingency Planning Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
CP-2	Contingency Plan	The organization: a. Develops a contingency plan for the information system that: • Identifies essential missions and business functions and associated contingency requirements; • Provides recovery objectives, restoration priorities, and metrics; • Addresses contingency roles, responsibilities, assigned individuals with contact information; • Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; • Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and • Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to an organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements; • *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 FedRAMP personnel.* c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system *at least annually*; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to an organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.

		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 FedRAMP personnel.
CP-3	Contingency Training	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training *at least annually*.
CP-4	Contingency and Plan Testing and Exercises	The organization: a. Tests and/or exercises the contingency plan for the information system *at least annually for moderate impact systems; at least every three years for low impact systems* using *functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems* to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. *The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB.*
CP-9	Information System Backup	The organization: a. Conducts backups of user-level information contained in the information system: *incremental, daily and full, weekly*; • *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 JAB.* b. Conducts backups of system-level information contained in the information system: *incremental, daily and full, weekly*; • *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 JAB.* c. Conducts backups of information system documentation including security-related documentation *incremental, daily and weekly, full*; and • *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 JAB.* d. Protects the confidentiality and integrity of backup information at the storage location. *The service provider shall determine what elements of the cloud environment require the Information System Backup control. The cloud environment elements requiring Information System Backup are approved and accepted by the JAB.* *The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check. The verification and periodicity of the Information System Backup are approved and accepted by the JAB.*
CP-10	Information System Recovery and Reconstitution	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

4.1.7 Identification and Authentication (IA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
IA-1	Identification and Authentication Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
IA-2	Identification and Authentication (Organizational Users)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
IA-2 (1)	Identification and Authentication (Organizational Users)	The information system uses multifactor authentication for network access to privileged accounts.
IA-4	Identifier Management	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier;

		b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for *at least two years*; and e. Disabling the user identifier *after ninety days for user identifiers*. *The service provider defines time period of inactivity for device identifiers. The time period is approved and accepted by JAB.*
IA-5	Authenticator Management	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators *every sixty days*; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.
IA-5 (1)	Authenticator Management	The information system, for password-based authentication: a. Enforces minimum password complexity of *case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters*; b. Enforces *at least one or as determined by the information system (where possible)* changed characters when new passwords are created; c. Encrypts passwords in storage and in transmission; d. Enforces password minimum and maximum lifetime restrictions of *one day minimum, sixty day maximum*; and e. Prohibits password reuse for *24* generations
IA-6	Authenticator Feedback	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
IA-7	Cryptographic Module Authentication	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
IA-8	Identification and Authentication (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

4.1.8 Incident Response (IR) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
IR-1	Incident Response Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
IR-2	Incident Response Training	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training *at least annually*.
IR-4	Incident Handling	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. *The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.*

IR-5	Incident Monitoring	The organization tracks and documents information system security incidents.
IR-6	Incident Reporting	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within *US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)*; and b. Reports security incident information to designated authorities.
IR-7	Incident Response Assistance	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.
IR-8	Incident Response Plan	The organization: a. Develops an incident response plan that: • Provides the organization with a roadmap for implementing its incident response capability; • Describes the structure and organization of the incident response capability; • Provides a high-level approach for how the incident response capability fits into the overall organization; • Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; • Defines reportable incidents; • Provides metrics for measuring the incident response capability within the organization. • Defines the resources and management support needed to effectively maintain and mature an incident response capability; and • Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to an organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements; • *The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.* c. Reviews the incident response plan at least annually; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to an organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements. *The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.*

4.1.9 Maintenance (MA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
MA-1	System Maintenance Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
MA-2	Controlled Maintenance	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
MA-4	Non-Local Maintenance	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
MA-5	Maintenance	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized

	Personnel	maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

4.1.10 Media Protection (MP) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
MP-1	Media Protection Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
MP-2	Media Access	The organization restricts access to organization-defined types of digital and non-digital media to organization-defined list of authorized individuals using organization-defined security measures. *The service provider defines types of digital and non-digital media. The media types are approved and accepted by the JAB.* *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 JAB.* *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 JAB.*
MP-6	Media Sanitization	The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

4.1.11 Physical and Environmental Protection (PE) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
PE-1	Physical and environmental protection policy and procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
PE-2	Physical Access Authorizations	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials *at least annually*, removing from the access list personnel no longer requiring access.
PE-3	Physical Access Control	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices *at least annually*; and g. Changes combinations and keys *at least annually* and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
PE-6	Monitoring Physical Access	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs *at least semi-annually*; and c. Coordinates results of reviews and investigations with the organization's incident response capability.

PE-7	Visitor Control	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
PE-8	Access Records	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records *at least monthly*.
PE-12	Emergency Lighting	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
PE-13	Fire Protection	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
PE-14	Temperature and Humidity Controls	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at *consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments*; and b. Monitors temperature and humidity levels *continuously*. *The service provider measures temperature at server inlets and humidity levels by dew point.*
PE-15	Water Damage Protection	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
PE-16	Delivery and Removal	The organization authorizes, monitors, and controls *all information systems* entering and exiting the facility and maintains records of those items.

4.1.12 Planning (PL) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
PL-1	Security Planning Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
PL-2	System Security Plan	The organization: a. Develops a security plan for the information system that: • Is consistent with the organization's enterprise architecture; • Explicitly defines the authorization boundary for the system; • Describes the operational context of the information system in terms of missions and business processes; • Provides the security categorization of the information system including supporting rationale; • Describes the operational environment for the information system; • Describes relationships with or connections to other information systems; • Provides an overview of the security requirements for the system; • Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and • Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system *at least annually*; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
PL-4	Rules of Behavior	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
PL-5	Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

4.1.13 Personnel Security (PS) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
PS-	Personnel	The organization develops, disseminates, and reviews/updates *at least annually*:

1	Security Policy and Procedures	a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
PS-2	Position Categorization	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations *at least every three years*.
PS-3	Personnel Screening	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to required conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening. *For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance.* *For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions*
PS-4	Personnel Termination	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.
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 organization-defined transfer or reassignment actions *within five days*. *The service provider defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the JAB.*
PS-6	Access Agreements	The organization: a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements *at least annually*.
PS-7	Third-Party Personnel Security	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.
PS-8	Personnel Sanctions	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

4.1.14 Risk Assessment (RA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
RA-1	Risk Assessment Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
RA-2	Security Categorization	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
RA-3	Risk Assessment	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

		b. Documents risk assessment results in a *security assessment report*; c. Reviews risk assessment results *at least every three years or when a significant change occurs*; and • *Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.* d. Updates the risk assessment *at least every three years or when a significant change occurs* or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. *Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.*
RA-5	Vulnerability Scanning	The organization: a. Scans for vulnerabilities in the information system and hosted applications *quarterly for operating system, web application, and database scans (as applicable)* and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: • Enumerating platforms, software flaws, and improper configurations; • Formatting and making transparent, checklists and test procedures; and • Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and • *High-risk vulnerabilities mitigated within thirty days* • *Moderate risk vulnerabilities mitigated within ninety days* e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

4.1.15 System and Services Acquisition (SA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
SA-1	System and Services Acquisition Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
SA-2	Allocation of Resources	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.
SA-3	Life Cycle Support	The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities
SA-4	Acquisitions	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.
SA-5	Information System Documentation	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: • Secure configuration, installation, and operation of the information system; • Effective use and maintenance of security features/functions; and • Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the

		information system that describes: • User-accessible security features/functions and how to effectively use those security features/functions; • Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and • User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
SA-6	Software Usage Restrictions	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
SA-7	User-Installed Software	The organization enforces explicit rules governing the installation of software by users.
SA-9	External Information System Services	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.

4.1.16 System and Communications Protection (SC) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
SC-1	System and Communications Protection Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
SC-5	Denial of Service Protection	The information system protects against or limits the effects of denial of service attacks. *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 of denial of service attack types is approved and accepted by JAB.*
SC-7	Boundary Protection	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
SC-12	Cryptographic Key Establishment and Management	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.
SC-13	Use of Cryptography	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
SC-14	Public Access Protections	The information system protects the integrity and availability of publicly available information and applications.
SC-15	Collaborative Computing Devices	The information system: a. Prohibits remote activation of collaborative computing devices with *no exceptions*; and b. Provides an explicit indication of use to users physically present at the devices.
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.
SC-20	Secure Name /Address	The information system, when operating as part of a distributed, hierarchical namespace, provides

(1)	Resolution Service (Authoritative Source)	the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

4.1.17 System and Information Integrity (SI) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Low Parameters*
S1-1	System and Information Integrity Policy and Procedures	The organization develops, disseminates, and reviews/updates *at least annually*: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
S1-2	Flaw Remediation	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.
SI-3	Malicious Code Protection	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: • Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or • Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: • Perform periodic scans of the information system *at least weekly* and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and • *Block or quarantine malicious code, send an alert to the administrator, and send an alert to FedRAMP* d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
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; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to *all staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP*; and • *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 FedRAMP personnel.* d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
SI-12	Information Output Handling and Retention	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

4.2 FedRAMP Controls for Moderate Certification

In addition to meeting all FedRAMP Low requirements (Section 3.1), providers seeking FedRAMP moderate certification must meet the following additional requirements. These additional requirements are selected from the NIST 800-53 [63] requirements and with additional parameters above defined in FedRAMP guidance [62]. The following tables list those requirements, beyond FedRAMP Low requirements, that providers must meet for FedRAMP Moderate accreditation.

4.2.1 Access Control Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
AC-2 (1)	Account Management	The organization employs automated mechanisms to support the management of information system accounts.
AC-2 (2)	Account Management	The information system automatically terminates temporary and emergency accounts after no more *than ninety days for temporary and emergency account types*.
AC-2 (3)	Account Management	The information system automatically disables inactive accounts after *ninety days for user accounts*.
AC-2 (4)	Account Management	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.
AC-2 (7)	Account Management	The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and b. Tracks and monitors privileged role assignments.
AC-3 (3)	Access Enforcement	The information system enforces *role-based access control* over all *users and resources* where the policy rule set for each policy specifies: a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and b. Required relationships among the access control information to permit access. *The service provider:* • *Assigns user accounts and authenticators in accordance within service provider's role-based access control policies;* • *Configures the information system to request user ID and authenticator prior to system access; and* • *Configures the databases containing federal information in accordance with service provider's security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.*
AC-4	Information Flow Enforcement	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
AC-5	Separation of Duties	The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.
AC-6	Least Privilege	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.
AC-6 (1)	Least Privilege	The organization *defines the list of security functions* deployed in hardware, software, and firmware. *The list of functions is approved and accepted by the JAB.*
AC-6 (2)	Least Privilege	The organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.
AC-10	Concurrent Session Control	The information system limits the number of concurrent sessions for each system account to *one session*.
AC-11	Session Lock	The information system: a. Prevents further access to the system by initiating a session lock after *fifteen minutes* 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.
AC-11 (1)	Session Lock	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 *for IaaS and PaaS*.
AC-14 (1)	Permitted Actions without Identification or Authentication	The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.
AC-16	Security Attributes	*If the service provider offers the capability of defining security attributes* to information in storage, in process, and in transmission, *then the security attributes need to be approved and accepted by JAB*.
AC-17 (1)	Remote Access	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

AC-17 (2)	Remote Access	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.
AC-17 (3)	Remote Access	The information system routes all remote accesses through a limited number of managed access control points.
AC-17 (4)	Remote Access	The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.
AC-17 (5)	Remote Access	The organization monitors for unauthorized remote connections to the information system *continuously, real time*, and takes appropriate action if an unauthorized connection is discovered.
AC-17 (7)	Remote Access	For remote sessions that access security functions and security-relevant information, the *service provider defines the list of security functions and security relevant information, which is approved and accepted by the JAB,* and ensures that the remote sessions are audited.
AC-17 (8)	Remote Access	*Networking protocols implemented by the service provider are approved and accepted by JAB.* The organization disables *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* protocols. *Exceptions to restricted networking protocols are granted for explicitly identified information system components in support of specific operational requirements.*
AC-18 (1)	Wireless Access	The information system protects wireless access to the system using authentication and encryption.
AC-18 (2)	Wireless Access	The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points *at least quarterly*, and takes appropriate action if an unauthorized connection is discovered.
AC-19 (1)	Access Control for Mobile Devices	The organization restricts the use of writable, removable media in organizational information systems.
AC-19 (2)	Access Control for Mobile Devices	The organization prohibits the use of personally owned, removable media in organizational information systems.
AC-19 (3)	Access Control for Mobile Devices	The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.
AC-20 (1)	Use of External Information Systems	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system
AC-20 (2)	Use of External Information Systems	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

4.2.2 Audit and Accountability (AU) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
AU-2 (3)	Auditable Events	The organization reviews and updates the list of auditable events *annually or whenever changes in the threat environment are communicated to the service provider by the JAB.*
AU-2 (4)	Auditable Events	The organization includes execution of privileged functions in the list of events to be audited by the information system. *The service provider configures the auditing features of operating systems, databases, and applications to record security-related events, to include logon/logoff and all failed access attempts.*
AU-3 (1)	Content of Audit Records	*The service provider defines audit record types. The audit record types are approved and accepted by the JAB. For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.* The information system includes the following in the audit records for audit events identified by type, location, or subject: • *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*
AU-6 (1)	Audit Review, Analysis, and Reporting	The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
AU-6 (3)	Audit Review, Analysis, and Reporting	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
AU-7	Audit Reduction and Report Generation	The information system provides an audit reduction and report generation capability.
AU-7 (1)	Audit Reduction and Report Generation	The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.
AU-8 (1)	Time Stamps	The information system synchronizes internal information system clocks *at least hourly* with *http://tf.nist.gov/tf-cgi/servers.cgi* *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.* *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 (2)	Protection of Audit Information	The information system backs up audit records *at least weekly* onto a different system or media than the system being audited.
AU-10	Non-Repudiation	The information system protects against an individual falsely denying having performed a particular action.
AU-10 (5)	Non-Repudiation	The organization implements digital signatures with *FIPS-140-2 validate cryptography (e.g., DoD PKI Class 3 or 4 tokens) for service offerings that include Software as a Service (SaaS) with email.*

4.2.3 Assessment and Authorization (CA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
CA-7 (2)	Continuous Monitoring	The organization plans, schedules, and conducts assessments *annually, unannounced, penetration testing in-depth monitoring* to ensure compliance with all vulnerability mitigation procedures.

4.2.4 Configuration Management (CM) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
CM-2 (1)	Baseline Configuration	The organization reviews and updates the baseline configuration of the information system: a. *annually*; b. When required due to *a significant change*; and c. As an integral part of information system component installations and upgrades. *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 JAB.*
CM-2 (3)	Baseline Configuration	The organization retains older versions of baseline configurations as deemed necessary to support rollback.
CM-2 (5)	Baseline Configuration	The organization: a. *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 JAB.* The provider develops and maintains these software programs; and b. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.
CM-3	Configuration Change Control	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. *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 JAB. The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB.*
CM-5	Access Restrictions for Change	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
CM-5 (1)	Access Restrictions for Change	The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
CM-5 (5)	Access Restrictions for Change	The organization: a. Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and b. Reviews and reevaluates information system developer/integrator privileges *at least quarterly*.
CM-6 (1)	Configuration Settings	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
CM-6 (3)	Configuration Settings	The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.
CM-7 (1)	Least Functionality	The organization reviews the information system *at least quarterly* to identify and eliminate unnecessary functions, ports, protocols, and/or services.
CM-8 (1)	Information System Component Inventory	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
CM-8 (3)	Information System Component Inventory	The organization: a. Employs automated mechanisms *continuously, using automated mechanisms with a maximum five-minute delay in detection* to detect the addition of unauthorized components/devices into the information system; and b. Disables network access by such components/devices or notifies designated organizational officials.
CM-8 (5)	Information System Component Inventory	The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.
CM-9	Configuration Management Plan	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.

4.2.5 Contingency Planning Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
CP-2 (1)	Contingency Plan	The organization coordinates contingency plan development with organizational elements responsible for related plans.
CP-2 (2)	Contingency Plan	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
CP-4 (1)	Contingency Plan Testing and Exercises	The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.
CP-6	Alternate Storage Site	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.
CP-6 (1)	Alternate Storage Site	The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.
CP-6 (3)	Alternate Storage Site	The organization identifies potential accessibility problems to the alternate storage site in the event of

		an area-wide disruption or disaster and outlines explicit mitigation actions.
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 an organization-defined time period consistent with recovery time objectives when the primary processing capabilities are unavailable; and • *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 JAB.* b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.
CP-7 (1)	Alternate Processing Site	The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.
CP-7 (2)	Alternate Processing Site	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
CP-7 (3)	Alternate Processing Site	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.
CP-7 (5)	Alternate Processing Site	The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.
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 an organization-defined time period when the primary telecommunications capabilities are unavailable. *The service provider defines a time period consistent with the business impact analysis. The time period is approved and accepted by the JAB.*
CP-8 (1)	Telecommunications Services	The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
CP-8 (2)	Telecommunications Services	The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.
CP-9 (1)	Information System Backup	The organization tests backup information *at least annually* to verify media reliability and information integrity.
CP-9 (3)	Information System Backup	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.
CP-10 (2)	Information System Recovery and Reconstitution	The information system implements transaction recovery for systems that are transaction-based.
CP-10 (3)	Information System Recovery and Reconstitution	The organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution to a known state. *The service provider defines circumstances that can inhibit recovery and reconstitution to a known state in accordance with the contingency plan for the information system and business impact analysis.*

4.2.6 Identification and Authentication (IA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
IA-2 (2)	Identification and Authentication (Organizational Users)	The information system uses multifactor authentication for network access to non-privileged accounts.
IA-2 (3)	Identification and Authentication (Organizational Users)	The information system uses multifactor authentication for local access to privileged accounts.
IA-2 (8)	Identification and Authentication (Organizational Users)	The information system uses organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.

		The service provider defines replay-resistant authentication mechanisms. The mechanisms are approved and accepted by the JAB.
IA-3	Device Identification and Authentication	The information system uniquely identifies and authenticates an organization defined list of specific and/or types of devices before establishing a connection. *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 JAB.*
IA-4 (4)	Identifier Management	The organization manages user identifiers by uniquely identifying the user as a *contractor and/or foreign national*.
IA-5 (2)	Authenticator Management	The information system, for PKI-based authentication: a. Validates certificates by constructing a certification path with status information to an accepted trust anchor; b. Enforces authorized access to the corresponding private key; and c. Maps the authenticated identity to the user account.
IA-5 (3)	Authenticator Management	The organization requires that the registration process to receive *HSPD12 smart cards* be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).
IA-5 (6)	Authenticator Management	The organization protects authenticators commensurate with the classification or sensitivity of the information accessed.
IA-5 (7)	Authenticator Management	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

4.2.7 Incident Response (IR) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
IR-3	Incident Response Testing and Exercises	The organization tests and/or exercises the incident response capability for the information system *annually* using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results. *The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended).* *The service provider provides test plans to FedRAMP annually. Test plans are approved and accepted by the JAB prior to test commencing.*
IR-4 (1)	Incident Handling	The organization employs automated mechanisms to support the incident handling process.
IR-6 (1)	Incident Reporting	The organization employs automated mechanisms to assist in the reporting of security incidents.
IR-7 (1)	Incident Response Assistance	The organization employs automated mechanisms to increase the availability of incident response-related information and support.
IR-7 (2)	Incident Response Assistance	The organization: a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and b. Identifies organizational incident response team members to the external providers.

4.2.8 Maintenance (MA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
MA-2 (1)	Controlled Maintenance	The organization maintains maintenance records for the information system that include: a. Date and time of maintenance; b. Name of the individual performing the maintenance; c. Name of escort, if necessary; d. A description of the maintenance performed; and e. A list of equipment removed or replaced (including identification numbers, if applicable).
MA-3	Maintenance Tools	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.
MA-3 (1)	Maintenance Tools	The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.
MA-3	Maintenance	The organization checks all media containing diagnostic and test programs for malicious code before the media

(2)	Tools	are used in the information system.
MA-3 (3)	Maintenance Tools	The organization prevents the unauthorized removal of maintenance equipment by one of the following: a. verifying that there is no organizational information contained on the equipment; b. sanitizing or destroying the equipment; c. retaining the equipment within the facility; or d. obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.
MA-4 (1)	Non-Local Maintenance	The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.
MA-4 (2)	Non-Local Maintenance	The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.
MA-6	Timely Maintenance	The organization obtains maintenance support and/or spare parts for an organization-defined list of security-critical information system components and/or key information technology components within an organization-defined time period of failure. *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 JAB.* *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 JAB.*

4.2.9 Media Protection (MP) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
MP-2 (1)	Media Access	The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.
MP-3	Media Marking	The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts *no removable media types* from marking.
MP-4	Media Storage	The organization: a. Physically controls and securely stores *magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks* within organization-defined controlled areas using: *for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secure storage in locked cabinets or safes*; • *The service provider defines controlled areas within facilities where the information and information system reside.* b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
MP-4 (1)	Media Storage	The organization employs cryptographic mechanisms to protect information in storage.
MP-5	Media Transport	The organization: a. Protects and controls *magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks* during transport outside of controlled areas using: *for digital media, encryption using a FIPS 140-2 validated encryption module*; • *The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB.* b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel.
MP-5 (2)	Media Transport	The organization documents activities associated with the transport of information system media.
MP-5 (4)	Media Transport	The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
MP-6 (4)	Media Sanitization	The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.

4.2.10 Physical and Environmental Protection (PE) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
PE-4	Access Control for Transmission Medium	The organization controls physical access to information system distribution and transmission lines within organizational facilities.
PE-5	Access Control for Output Devices	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
PE-6 (1)	Monitoring Physical Access	The organization monitors real-time physical intrusion alarms and surveillance equipment.
PE-7 (1)	Visitor Control	The organization escorts visitors and monitors visitor activity, when required.
PE-9	Power Equipment and Power Cabling	The organization protects power equipment and power cabling for the information system from damage and destruction.
PE-10	Emergency Shutoff	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in organization-defined locations by information system or system component to facilitate safe and easy access for personnel; and • *The service provider defines emergency shutoff switch locations. The locations are approved and accepted by the JAB.* c. Protects emergency power shutoff capability from unauthorized activation.
PE-11	Emergency Power	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
PE-13 (1)	Fire Protection	The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.
PE-13 (2)	Fire Protection	The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.
PE-13 (3)	Fire Protection	The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.
PE-17	Alternate Work Site	The organization: a. Employs organization-defined management, operational, and technical information system security controls at alternate work sites; • *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 JAB.* b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.
PE-18	Location of Information System Components	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

4.2.11 Planning (PL) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
PL-6	Security-Related Activity Planning	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

4.2.12 Risk Assessment (RA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
RA-5 (1)	Vulnerability Scanning	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.
RA-5 (2)	Vulnerability Scanning	The organization updates the list of information system vulnerabilities scanned *continuously, before each scan* or when new vulnerabilities are identified and reported.
RA-5 (3)	Vulnerability Scanning	The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

RA-5 (6)	Vulnerability Scanning	The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.
RA-5 (9)	Vulnerability Scanning	The organization employs an independent penetration agent or penetration team to: a. Conduct a vulnerability analysis on the information system; and b. Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

4.2.13 System and Services Acquisition (SA) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
SA-4 (1)	Acquisitions	The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.
SA-4 (4)	Acquisitions	The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.
SA-4 (7)	Acquisitions	The organization: a. Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists; and b. Requires, if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.
SA-5 (1)	Information System Documentation	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.
SA-5 (3)	Information System Documentation	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.
SA-8	Security Engineering Principles	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.
SA-9 (1)	External Information System Services	The organization: a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by *the Joint Authorization Board (JAB)*. • *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 JAB.*
SA-10	Developer Configuration Management	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.
SA-11	Developer Security Testing	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.
SA-11 (1)	Developer Security Testing	The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis. *The service provider submits a code analysis report as part of the authorization package and updates the report in any reauthorization actions.* *The service provider documents, in the Continuous Monitoring Plan, how newly developed code for the*

		information system is reviewed.
SA-12	Supply Chain Protection	The organization protects against supply chain threats by employing an organization-defined list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy. *The service provider defines a list of measures to protect against supply chain threats. The list of protective measures is approved and accepted by JAB.*

4.2.14 System and Communications Protection (SC) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
SC-2	Application Partitioning	The information system separates user functionality (including user interface services) from information system management functionality.
SC-4	Information in Shared Resources	The information system prevents unauthorized and unintended information transfer via shared system resources.
SC-6	Resource Priority	The information system limits the use of resources by priority.
SC-7 (1)	Boundary Protection	The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. *The service provider and service consumer ensure that federal information (other than unrestricted information) being transmitted from federal government entities to external entities using information systems providing cloud services is inspected by TIC processes.*
SC-7 (2)	Boundary Protection	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)	Boundary Protection	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)	Boundary Protection	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 *at least annually*; and f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.
SC-7 (5)	Boundary Protection	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 (7)	Boundary Protection	The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.
SC-7 (8)	Boundary Protection	The information system routes internal communications traffic to defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices. *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 JAB.*
SC-7 (12)	Boundary Protection	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.
SC-7 (13)	Boundary Protection	The organization isolates key information security tools, mechanisms, and support components from other internal information system components via physically separate subnets with managed interfaces to other portions of the system. *The service provider defines key information security tools, mechanisms, and support components associated with system and security administration, and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.*
SC-7 (18)	Boundary Protection	The information system fails securely in the event of an operational failure of a boundary protection device.
SC-8	Transmission Integrity	The information system protects the integrity of transmitted information.

SC-8 (1)	Transmission Integrity	The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.
SC-9	Transmission Confidentiality	The information system protects the confidentiality of transmitted information.
SC-9 (1)	Transmission Confidentiality	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by organizational defined alternative physical measures. *The service provider must implement a hardened or alarmed carrier Protective Distribution System (PDS) when transmission confidentiality cannot be achieved through cryptographic mechanisms.*
SC-10	Network Disconnect	The information system terminates the network connection associated with a communications session at the end of the session or after *thirty minutes of inactivity for all RAS-based sessions; thirty to sixty minutes of inactivity for non-interactive users.* • *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: organization-defined security functions to include at a minimum, information system authentication and re-authentication. *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 JAB.*
SC-12 (2)	Cryptographic Key Establishment and Management	The organization produces, controls, and distributes symmetric cryptographic keys using *NIST-approved* key management technology and processes.
SC-12 (5)	Cryptographic Key Establishment and Management	The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key. • *The service provider supports the capability to produce, control, and distribute asymmetric cryptographic keys.*
SC-13 (1)	Use of Cryptography	The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.
SC-17	Public Key Infrastructure Certificates	The organization issues public key certificates under an organization defined certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. • *The service provider defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the JAB.*
SC-18	Mobile Code	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.
SC-19	Voice Over Internet Protocol	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.
SC-21	Secure Name/ Address Resolution Service (Recursive or Caching Resolver)	The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.
SC-22	Architecture and Provisioning for Name/Address Resolution Service	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
SC-23	Session Authenticity	The information system provides mechanisms to protect the authenticity of communications sessions.
SC-28	Protection of Information at Rest	The information system protects the confidentiality and integrity of information at rest. • *The organization supports the capability to use cryptographic mechanisms to protect information at rest*
SC-30	Virtualization Techniques	The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.
SC-32	Information System	The organization partitions the information system into components residing in separate physical

	Partitioning	domains (or environments) as deemed necessary.

4.2.15 System and Information Integrity (SI) Requirements

ID	Control Name	NIST 800-53 Control with *FedRAMP Moderate Parameters*
SI-2 (2)	Flaw Remediation	The organization employs automated mechanisms *at least monthly* to determine the state of information system components with regard to flaw remediation.
SI-3 (1)	Malicious Code Protection	The organization centrally manages malicious code protection mechanisms.
SI-3 (2)	Malicious Code Protection	The information system automatically updates malicious code protection mechanisms (including signature definitions).
SI-3 (3)	Malicious Code Protection	The information system prevents non-privileged users from circumventing malicious code protection capabilities.
SI-4	Information System Monitoring	The organization: a. Monitors events on the information system and detects information system attacks; • *Monitoring objectives include: 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* 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 (2)	Information System Monitoring	The organization employs automated tools to support near real-time analysis of events.
SI-4 (4)	Information System Monitoring	The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.
SI-4 (5)	Information System Monitoring	The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: • *protected information system files or directories have been modified without notification from the appropriate change/configuration management channels;* • *information system performance indicates resource consumption that is inconsistent with expected operating conditions;* • *auditing functionality has been disabled or modified to reduce audit visibility;* • *audit or log records have been 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 that are 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 that are outside of the baseline system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose* *The service provider defines additional compromise indicators as needed.* *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.*
SI-4 (6)	Information System Monitoring	The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.
SI-6	Security functionality verification	The information system verifies the correct operation of security functions *upon system startup and/or restart*; upon command by user with appropriate privilege; *and periodically every ninety days*

		and *notifies system administrators* when anomalies are discovered.
SI-7	Software and Information Integrity	The information system detects unauthorized changes to software and information.
SI-7 (1)	Software and Information Integrity	The organization reassesses the integrity of software and information by performing *at least monthly* integrity scans of the information system.
SI-8	Spam Protection	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.
SI-9	Information Input Restrictions	The organization restricts the capability to input information to the information system to authorized personnel.
SI-10	Information Input Validation	The information system checks the validity of information inputs.
SI-11	Error Handling	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing *user name and password combinations; attributes used to validate a password reset request (e.g. security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings)* in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.

4.3 FedRAMP Ongoing Assessment & Authorization Requirements

The purpose of the ongoing assessment and authorization process is to ensure that security controls implemented during the security authorization remain effective [67]. The process consists of three steps, shown in the table below. The approach is based on NIST SP 800-137 [68].

Table 7: FedRAMP specifies three Ongoing Assessment and Authorization steps [67].

Step	Description
Operational Visibility	Provides visibility into security control implementations through: a. Automated data feeds b. Periodically submitted specific control evidentiary artifacts c. Annual self-attestation reports
Change Control Process	Relates to any changes or proposed changes that significantly impact the CSP's ability to meet FedRAMP requirements, CSP management oversight, and its Plan of Action and Milestones (POA&Ms).
Incident Response	Focuses on new risks and vulnerabilities that impact a FedRAMP authorized system. It also includes all responses and mitigation activities needed to return the system to a secure state and maintain that security.

4.3.1 Step 1: Operational Visibility Requirements

Cloud service providers must provide three types of information:

Requirement	Description
Automated Data Feeds	CSPs are required to submit automated data feeds to Federal agencies and must work with Federal agencies to ensure these feeds are received [68]. • The feeds include CyberScope data • Federal agencies submit CyberScope feeds to DHS
Self-Attestation Review	CSPs must: a. annually re-assess a subset of security controls, and • Re-assessments must be performed by FedRAMP accepted 3PAOs. b. CSPs must submit an annual self-attestation report that certifies all controls are working properly.

Periodic Artifacts	The CSP must be able to provide period evidentiary artifacts for specific controls.

4.3.2 Step 2: Change Control Requirements

When a provider makes significant changes to "the scope of an approved Provisional Authorization or impact the authorization boundary" they must follow the change control requirements outlined below [68].

Requirement	Description
Change Documentation	The provider must deliver information to FedRAMP on any changes or proposed changes that impact the CSP's ability to meet FedRAMP requirements by submitting an updated Configuration Management Plan and any other documents that capture significant changes, such as the SSP and IT Contingency Plan [68]. a. FedRAMP and Federal agencies will use this information to make a risk based decision about the risks associated with the changes. b. These include, but are not limited to: • Changes In the CSP's point of contact with FedRAMP • Changes in Risk posture • Changes to applications residing on the cloud system • Changes to the cloud system infrastructure
Review Planned Changes	If FedRAMP determines that any change will add residual risk or change a user agency's responsibilities the CSP must review the planned implementation with the Government ISSO for provisional authorization. • The review will include recommendations from the ISSO and Authorizing Authority. • If the change creates risks that the JAB finds unacceptable, the Provisional Authorization will either be updated to reflect revisions to the POA&M, additional conditions, or revocation of Provisional Authorization (if implemented).
Change Documentation	After any significant change the provider must: a. Document any impacted security controls in the SSP b. Undergo reassessment by the 3PAO c. Update other documentation provided to FedRAMP • This includes security impact analysis artifacts • FedRAMP will notify user agencies of the changes. d. Update POA&M that is submitted and reviewed quarterly by the FedRAMP ISSO. • The ISSO will determine if the changes violate FedRAMP compliance or introduce an unacceptable level of risk.

4.3.3 Step 3: Incident Response

Requirement	Description
Incident Response Plan	The CSP security authorization package requires CPSs to provide incident response plans in accordance with Federal policies, such as OMB M-07-16 and NIST Special Publication 800-61. [68]
Notification	In the event of a security incident, the provider must notify US-CERT and the impacted Federal agency (user) Security Operation Centers (SOCs). [68] • FedRAMP and US-CERT will coordinate a response and will summarize any findings in an Incident Report.
Prevention	The provider may be notified of actions required to prevent future incidents. The provider must record these actions in their POA&M and monitored.
Provisional Authorization Review	The provider must cooperate with FedRAMP, as directed, for serious incidents that initiate a review of a provider's authorization.

5 FedRAMP Plus Certifications

As cloud adoption rapidly increases amongst U.S. government organizations, many are formalizing additional requirements, beyond FedRAMP, that cloud service providers must also meet. Since FedRAMP authorization is mandatory to support federal organizations, the additional requirements are generically referred to as "FedRAMP Plus". In many instances, these organizations have stood up their own authorization process and bodies, similar to the FedRAMP JAB.

As of March, 2014 few agencies have formally outlined their FedRAMP Plus requirements. DISA is an exception and has taken the lead in defining requirements for all Department of Defense (DoD) organizations. DISA has also released the most complete requirements definition, which are currently in draft version. Other U.S. federal government organizations are actively exploring and adopting cloud computing, including the FAA and others listed in the figure above.

The following sections explore the DISA draft requirements to gain an understanding of what these additional requirements entail, how they will affect CSPs, and where pitfalls may exist. Since DISA requirements will apply to all DoD organizations, it also offers insight into standards that will affect a large number of cloud customers and CSPs.

5.1 FedRAMP Plus DISA Certification

DISA defines six impact levels based on data type and impact of a compromise on the confidentiality, integrity, or availability [59]. The matrix below outlines and defines each of these factors.

Table 8: DISA outlines four basic data types and three levels of risk for confidentiality, integrity, and availability [59].

Data Type	Impact	Confidentiality	Integrity	Availability
Public Information - Information approved for unrestricted public dissemination.	**Low**	Unauthorized disclosure would have a limited adverse effect.	Unauthorized modification or destruction of information would have a limited adverse effect.	**Customer Defined**
Unclassified Private	**Moderate**	Unauthorized disclosure would have a serious adverse effect.	Unauthorized modification or destruction of information would have a serious adverse effect.	
Controlled Unclassified Information - Includes Export-Control, HIPAA, FOUO, LE Sensitive, Critical Infrastructure Information	**High**	Unauthorized disclosure would have a severe or catastrophic adverse effect.	Unauthorized modification or destruction of information would have a severe or catastrophic adverse effect.	
Classified - Up to SECRET.				

The six impact levels are defined in the table below. For each impact level, DISA has defined requirements for IaaS, PaaS, and SaaS providers [59]. These requirements are outlined, for each impact level and provider type, in the table below.

Table 9: Cloud providers must receive approval to operate at one or more impact levels, based on the data type and C-I-A requirements.

Impact Level	Data Type				Confidentiality	Integrity	Availability
	Public	Unclassified Private	Controlled Unclassified	Classified			
1	✓				N/A	Low	*Customer Defined*
2		✓			Low	Moderate	*Customer Defined*
3			✓		Low	Moderate	*Customer Defined*
4			✓		Moderate	Moderate	*Customer Defined*
5			✓		High	High	*Customer Defined*
6				✓	High	High	*Customer Defined*

No information was provided for impact level 1 or 2 and the only partial information was provided for impact level 6, including the statement that "only DoD CSPs are eligible to provide services for impact level 6" [59]. Our research will outline each of the requirements for impact levels 3, 4, and 5 and assess the likelihood that existing, major providers can meet these needs.

5.1.1 Understanding Certification Requirements

DISA provides a series of requirements that each cloud service provider must meet, based upon the impact level and the cloud model (i.e., IaaS, PaaS, or SaaS). This document only covers the processes required for a commercial cloud service provider to receive accreditation, the process for DoD cloud service providers (those operated by DoD entities) can be found in the DISA Cloud Security Model document in Section 4.2 [59].

The full scope of security requirements for certification of a cloud service provider consist of six components, outlined in the table below. [59] Each component consists of a series of controls that a cloud provider must demonstrate to receive accreditation.

Table 10: DISA requires cloud providers to meet six sets of requirements for accreditation.

Abbreviation	Component	Description
FedRAMP	Federal Risk and Authorization Management Program (FedRAMP)	Defines a set of controls for low and moderate impact level systems based on NIST SP800-53. CSPs must implement these controls and undergo a third party assessment to verify their correct implementation [59][61][62].
CNSSI 1253	Committee on National Security Systems Instruction (CNSSI) 1253 Controls	Defines security controls for National Security Systems (NSS). For impact levels 1 and 2 a tailored set of reduced security controls that more closely alight with FedRAMP are used. For impact levels 3-6 the full set of CNSSI 1253 controls apply and are tailored for each impact level.
A&A	Ongoing Authorization and Assessments	Based upon the FedRAMP continuous monitoring strategy. The DoD will review artifacts through the FedRAMP continuous monitoring process as well as any additional DoD-specific controls and will be used in annual re-authorization of CSPs [59].
C2 & NetOps	DoD Command and Control and Network Operations Integration	Any provider of cloud services will be integrated within the DoD Command and Control and Network Operations (NetOps) structure [59]. The required level of integration increases as the impact level increases. It covers the process for informing the government of a breach, specific steps taken to remedy the breach, notifications to affected individuals, and other special instructions.
AI	Architectural Integration	Consists of DoD specific security requirements that go beyond defined security controls. These requirements increase as the impact level increases [59].
PGO	Policy, Guidance, and Operational Constraints	Outlines a set of constraints, specific to each impact level, which the CSP must follow in regard to policy, guidance, and operations.

The specific details of each component that a CSP must satisfy differ by the impact level. For example, a CSP pursuing a level 1 accreditation must achieve FedRAMP authorization for “low impact level systems”, while a CSP pursuing level 3 accreditation must achieve FedRAMP authorization for “moderate impact level systems” [59].

This document consolidates all these requirements in the following sections. To build a list of all requirements first identify the table row containing your cloud model and (maximum) impact level, then assemble the requirements from each of the sections within that row.

Table 11: This table references sections of this document containing all requirements DISA cloud providers must meet.

Cloud Model	Impact Level	FedRAMP Controls	CNSSI 1253	A&A	C2 & NetOps	AI	PGO
IaaS	1	4.1					
	2	4.1					
	3	4.2	5.2.1, 5.2.2	4.3	5.2.1	5.4.1	5.5.1, 5.5.2
	4	4.2	5.2.1, 5.2.2	4.3	5.2.1, 5.2.2	5.4.1, 5.4.1	5.5.1, 5.5.2
	5	4.2	5.2.1, 5.2.2, 5.2.4, 5.2.5	4.3	5.2.1, 5.2.2	5.4.1, 5.4.2	5.5.1, 5.5.2
	6	4.2					
PaaS	1	4.1					
	2	4.1					
	3	4.2	5.2.1, 5.2.2	4.3	5.2.1	5.4.1	5.5.1, 5.5.3
	4	4.2	5.2.1, 5.2.2	4.3	5.2.1, 5.2.2	5.4.1, 5.4.3	5.5.1, 5.5.3
	5	4.2	5.2.1, 5.2.2, 5.2.4, 5.2.5	4.3	5.2.1, 5.2.2, 5.2.3	5.4.1, 5.4.3	5.5.1, 5.5.3
	6	4.2					
SaaS	1	4.1					

	2	4.1					
	3	4.2	5.2.1, 5.2.2, 5.2.3, 5.2.4	4.3	5.2.1	5.4.1	5.5.1, 5.5.4
	4	4.2	5.2.1, 5.2.2, 5.2.3, 5.2.4	4.3	5.2.1, 5.2.2	5.4.1, 5.4.3	5.5.1, 5.5.4
	5	4.2	5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5	4.3	5.2.1, 5.2.2, 5.2.3	5.4.1, 5.4.3	5.5.1, 5.5.4
	6	4.2					

5.2 CNSSI 1253 Controls

DISA also specifies a set of NIST 800-53 controls designed to meet CNSSI 1253 standards [64]. Many of these controls are the same as FedRAMP low/moderate requirements, some are modified, and others are added. For simplicity, we list those that are modified and those that are added in the sections below. Any DISA defined parameters in the ESCS Cloud Security Model Control Parameters Annex Version 1.1 [60] are outlined in *green*, FedRAMP requirements remain in *red*. DISA did not provide parameters for some controls; these are highlighted in the list below along with controls that appear to be incorrect and comments in parenthesis.

5.2.1 CNSSI 1253 Baseline Controls

The controls in this list replace those in the FedRAMP lists, typically with more stringent parameters, designed to meet CNSSI 1253 requirements. The cloud service provider is still expected to meet all other FedRAMP requirements not in this list.

CNSSI Baseline Controls			
Impact	**IaaS**	**PaaS**	**SaaS**
1	✓	✓	✓
2	✓	✓	✓
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓

ID	Control Name	Description
		AC – Access Control
AC-2	Account Management	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: i. temporary accounts that are no longer required; and ii. accounts of terminated or transferred users; i. Granting access to the system based on: iii. a valid access authorization; iv. intended system usage; and v. other attributes as required by the organization or associated missions/business functions j. Reviewing accounts *every 30 days*.
AC-2 (2)	Account Management	The information system automatically terminates temporary and emergency accounts after *24 hours*.
AC-2 (3)	Account Management	The information system automatically disables inactive accounts after: a. *35 days for SaaS DoD customer's user accounts* b. *35 days for IaaS and PaaS DoD SA's admin accounts* c. *The 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 ECSB DAA
AC-3 (3)	Access Enforcement	The information system enforces *role-based access control* over *all users and resources* where the policy rule set for each policy specifies: a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and b. Required relationships among the access control information to permit access. *The service provider:* • *Assigns user accounts and authenticators in accordance within service provider's role-based access control policies;* • *Configures the information system to request user ID and authenticator prior to system access; and* • *Configures the databases containing federal information in accordance with service provider's security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.*
AC-6 (1)		The organization explicitly authorizes access to *all privileged functions (e.g., System Administrator, Security Administrator, Database Administrator)* deployed in hardware, software, and firmware. • *The service provider defines the list of security functions. The list of functions is approved and accepted by the ECSB DAA.*
AC-10	Concurrent Session Control	The information system limits the number of concurrent sessions for each system account to: • *three sessions for privileged access and two sessions for non-privileged access or* • *one session* (this is the FedRAMP requirement, which is more stringent than the DISA requirement)
AC-11	Session Lock	The information system: a. Prevents further access to the system by initiating a session lock after *fifteen minutes, except to fulfill documented, AO approved and validated mission requirements*, 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.
AC-16	Security Attributes	*If the service provider offers the capability of defining security attributes* to information in storage, in process, and in transmission, *then attribution markings should include items such as classification, compartments, and handling instructions for classified and CUI data.* *If the service provider offers the capability of defining security attributes, then the security attributes need to be approved and accepted by the ECSB DAA.*
AC-17 (7)	Remote Access	The organization ensures that remote sessions for accessing *security functions and security relevant configuration settings* employ *session encryption (e.g., SSH or encrypted VPN) and session transcripts* and are audited.
AC-17 (8)	Remote Access	The organization disables *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* protocols. *Networking protocols implemented by the service provider are approved and accepted by ECSB DAA.* *Exceptions to restricted networking protocols are granted for explicitly identified information system components in support of specific operational requirements.*
AC-18 (2)		The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points *continuously*, and takes appropriate action if an unauthorized connection is discovered.
AC-19	Access Control for Mobile Devices	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies *physical / logical inspection, and remediation measures (before connection to the network)* to mobile devices returning from locations that the organization deems to be of significant risk in

		accordance with organizational policies and procedures. • *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.* • *The service provider defines inspection and preventative measures. The measures are approved and accepted by ECSB DAA.*
AC-22	Publicly Accessible Content	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information *at least quarterly or as new information is posted*; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.
AT – Awareness and Training		
AT-3	Security Training	The organization provides role-based security-related training: • before authorizing access to the system or performing assigned duties; • when required by system changes; and • *at least annually* thereafter.
AT-4	Security Training Records	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for: • *At least three years for Impact Levels 1 & 2* • *Five years or 5 years after completion of a specific training program for Impact Levels 3-6.*
AU – Audit and Accountability		
AU-2 (3)		The organization reviews and updates the list of auditable events *annually or whenever there is a change in the threat environment*. *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-6	Audit Review, Analysis, and Reporting	The organization: a. Reviews and analyzes information system audit records every *seven days or more frequently if required by an alarm event or anomaly* for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
AU-10 (5)		The organization implements digital signatures with *FIPS-Validated or NSA-approved cryptography as required by the classification level of the information system.* *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.* *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 *a minimum of 5 years for Sensitive Compartmented Information and Sources And Methods Intelligence information and a minimum of 1 year for all other information (Unclassified through Collateral Top Secret)* to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
AU-12	Audit Generation	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at *all information system components and network components where audit capability is deployed*; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and

		c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.
CA – Security Assessment and Authorization		
CA-5	Plan of Action and Milestones	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones *at least quarterly or more frequently as required upon an event or anomaly* based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
CA-6	Security Authorization	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization *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.* *A 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 systems. The types of changes are approved and accepted by the JAB.*
CA-7 (2)		The organization plans, schedules, and conducts assessments *annually, unannounced, penetration testing and in-depth monitoring, plus monthly announced scans* to ensure compliance with all vulnerability mitigation procedures.
CM – Configuration Management		
CM-2 (1)		The organization reviews and updates the baseline configuration of the information system: a. *annually*; b. When required due to *significant system or security relevant changes or security incidents/attacks occur, or upon receipt of USERCYBERCOM tactical orders/directives*; and c. As an integral part of information system component installations and upgrades. *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 JAB.*
CM-2 (5)		The organization: a. Develops and maintains an organization-defined list of software programs authorized to execute on the information system. The provider develops and maintains these software programs; and • *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 ECSB DAA.* b. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.
CM-3	Configuration Change Control	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. *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 ECSB DAA. The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the ECSB DAA.*
CM-5 (5)	Access Restrictions for Change	The organization: a. Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and b. Reviews and reevaluates information system developer/integrator privileges *monthly*.
CM-6	Configuration	The organization:

	Settings	a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using *DoD security configuration and/or implementation guidance (e.g., DoD STIGs, NSA configuration guides, CTOs, DTMs, etc.)* that reflect the most restrictive mode consistent with operational requirements; • *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). 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.shtmlrequirements derived from CTOs and DTMs will be provided via the customer's CNDSP* b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
CM-7	Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the functions, ports, protocols, and/or services *defined in the United States Government Configuration Baseline (USGBC) and/or the DoDI 8551.1 PPSM VAs and CAL*. *The service provider shall use the along with the DoDI 8551.1 PPSM VAs and CAL and Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. The list of prohibited or restricted functions, ports, protocols, and/or services are approved and accepted by the ECSB DAA.* *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)		The organization reviews the information system *every 30 days* to identify and eliminate unnecessary functions, ports, protocols, and/or services.
CM-8	Information System Component Inventory	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes organization-defined information deemed necessary to achieve effective property accountability; and • *The service provider defines information deemed necessary to achieve effective property accountability. Property accountability information are approved and accepted by the ECSB DAA.* • *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.* e. Is available for review and audit by designated organizational officials.
CP – Contingency Planning		
CP-2	Contingency Plan	The organization: a. Develops a contingency plan for the information system that: • Identifies essential missions and business functions and associated contingency requirements; • Provides recovery objectives, restoration priorities, and metrics; • Addresses contingency roles, responsibilities, assigned individuals with contact information; • Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; • Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and • Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to *key personnel and organizational elements identified in the contingency plan*; • *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.*

		c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system *at least annually*; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to *key personnel and organization elements identified in the contingency plan*.
CP-3	Contingency Training	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training *at least annually as defined in the contingency plan*.
CP-4	Contingency and Plan Testing and Exercises	The organization: a. Tests and/or exercises the contingency plan for the information system *at least annually for moderate impact systems; at least every three years for low impact systems* using *functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems* to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. *The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the ECSB DAA.*
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 an organization-defined time period consistent with recovery time objectives when the primary processing capabilities are unavailable; and • *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 ECSB DAA.* • *DoD preferred values are 12 hours (Availability Moderate) or 1 hour (Availability High) as defined in the contingency plan.* b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.
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 an organization-defined time period when the primary telecommunications capabilities are unavailable. *The service provider defines a time period consistent with the business impact analysis. The time period is approved and accepted by the ECSB DAA.*
CP-9 (1)		The organization tests backup information **not less than monthly, or as defined in the contingency plan** to verify media reliability and information integrity.
IA – Identification and Authentication		
IA-2 (8)		The information system uses organization-defined replay-resistant authentication mechanisms for network access to privileged accounts. *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 ECSB DAA.*
IA-3	Device Identification and Authentication	The information system uniquely identifies and authenticates an organization defined list of specific and/or types of devices before establishing a connection. *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 ECSB DAA.* *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: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for at least *1 year for user identifiers (DoD is not* e. *going to specify value for device identifier)*; and f. Disabling the user identifier *after ninety days for user identifiers*. *The service provider defines time period of inactivity for device identifiers. The time period is approved and*

		accepted by ECSB DAA.
IA-5	Authenticator Management	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators *every sixty days for passwords; 3 years for CAC/PKI certificate, 3 years for biometrics, if applicable*; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.
IA-5 (3)		The organization requires that the registration process to receive *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* be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).
IR – Incident Response		
IR-3	Incident Response Testing and Exercises	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 organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results. *The service provider provides test plans to DoD annually. Test plans are approved and accepted by the ECSB DAA 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: • *US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended) for impact level 1* • *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*; and b. Reports security incident information to designated authorities.
MP – Media Protection		
MP-2	Media Access	The organization restricts access to organization-defined types of digital and non-digital media to organization-defined list of authorized individuals using organization-defined security measures. *The service provider defines types of digital and non-digital media. The media types are approved and accepted by the ECSB DAA.* *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 ECSB DAA.* *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 ECSB DAA.*
MP-5	Media Transport	The organization: a. Protects and controls *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) during transport outside of controlled areas using:* • *FIPS 140-2 validated encryption (Impact Levels 2-5)* • *FIPS 140-2 validated encryption or NSA approved encryption IAW DoDI 5200.1R and other DoD defined security measures (Impact Level 6)* • *The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by ECSB DAA.* b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel.
PE – Physical and Environmental Protection		
PE-2	Physical Access Authorizations	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly

		accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials *monthly*, removing from the access list personnel no longer requiring access.
PE-3	Physical Access Control	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices *at least bi-annually*; and g. Changes combinations and keys *at least annually and as required by security relevant events* and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
PE-6	Monitoring Physical Access	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs *monthly*; and c. Coordinates results of reviews and investigations with the organization's incident response capability.
PE-10	Emergency Shutoff	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in organization-defined locations by information system or system component to facilitate safe and easy access for personnel; and • *The service provider defines emergency shutoff switch locations. The locations are approved and accepted by the ECSB DAA.* c. Protects emergency power shutoff capability from unauthorized activation.
PE-16	Delivery and Removal	The organization authorizes, monitors, and controls *all information system components* entering and exiting the facility and maintains records of those items.
PS – Personnel Security		
PS-2	Position Categorization	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations *at least annually*.
PS-3	Personnel Screening	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to *applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position required.* • *For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance.* • *For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year.* • *There is no reinvestigation for other moderate risk positions or any low risk positions*
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 *actions to ensure all system accesses no longer required are removed* within *24 hours*. *The service provider defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the ECSB DAA.*
RA – Risk Assessment		
RA-5	Vulnerability Scanning	The organization: a. Scans for vulnerabilities in the information system and hosted applications *monthly for operating system/infrastructure; quarterly for web application, and databases* and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: • Enumerating platforms, software flaws, and improper configurations;

		• Formatting and making transparent, checklists and test procedures; and • Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and • *High-risk vulnerabilities mitigated within thirty days* • *Moderate risk vulnerabilities mitigated within ninety days* e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). *An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.*
SA – System and Services Acquisition		
SA-9 (1)	External Information System Services	The organization: a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by the **DoD ECSB DAA**. • *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 ECSB DAA.*
SA-12	Supply Chain Protection	The organization protects against supply chain threats by employing an organization-defined list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy. *The service provider defines a list of measures to protect against supply chain threats. The list of protective measures is approved and accepted by ECSB DAA.*
SC – System and Communications Protection		
SC-5	Denial of Service Protection	The information system protects against or limits the effects of denial of service attacks. • *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 ECSB DAA.* • *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 (8)	Boundary Protection	The information system routes internal communications traffic to defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices. • *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 ECSB DAA.*
SC-10	Network Disconnect	The information system terminates the network connection associated with a communications session at the end of the session or after: • *Thirty minutes of inactivity for all RAS-based sessions; thirty to sixty minutes of inactivity for non-interactive users at Impact Level 1.* • *10 minutes in band management, 15 minutes for user sessions, except to fulfill documented and validated mission requirements for Impact Levels 2-6.* • *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: organization-defined security functions to include at a minimum, information system authentication and re-authentication. *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 ECSB DAA.*
SC-12 (2)	Cryptographic Key Establishment and Management	The organization produces, controls, and distributes symmetric cryptographic keys using the following key management technology and processes: • *NIST FIPS-Validated for Unclassified systems (Impact Levels 2-5)* • *NSA Approved/FIPS-Validated for Classified Systems (Impact Level 6)*

SC-15	Collaborative Computing Devices	The information system: a. Prohibits remote activation of collaborative computing devices with *no exceptions*; and b. Provides an explicit indication of use to users physically present at the devices. *The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.*
SC-17	Public Key Infrastructure Certificates	The organization issues public key certificates under an organization defined certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. *The service provider defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the ESCB DAA.*
SI – System and Information Integrity		
SI-2 (2)	Flaw Remediation	The organization employs automated mechanisms *continuously for endpoints; 30 days for internal network scans; annually for external scans* to determine the state of information system components with regard to flaw remediation.
SI-3	Malicious Code Protection	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: • Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or • Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: • Perform periodic scans of the information system *at least weekly* and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and • *Block or quarantine malicious code, send an alert to the administrator, and send an alert to USCYBERCOM via DoD customer's CNDSP, and send an alert to ECSB.* d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
SI-4	Information System Monitoring	The organization: a. Monitors events on the information system and detects information system attacks; • *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 ECSB DAA.* • *DoD Sensor placement and monitoring requirements are found in CJCSI 6510.01F* 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-6	Security functionality verification	The information system verifies the correct operation of security functions *upon system startup and/or restart*, upon command by user with appropriate privileges, and periodically *monthly* and *notifies system administrators* when anomalies are discovered.

5.2.2 CNSSI 1253 Additional Control Set 1

This additional control set applies to impact level 3-5.

CNSSI Additional Control Set 1			
Impact	**IaaS**	**PaaS**	**SaaS**
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓

Additional Control Set 1		
ID	**Control Name**	**Description**
AC-6 (5)	Least Privilege	The organization limits authorization to super user accounts on the information system to designated system administration personnel.
CA-7 (1)	Continuous Monitoring	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)	Security Impact Analysis	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)	Access Restrictions for Change	The organization limits privileges to change software resident within software libraries (including privileged programs).
IA-2 (5)	Identification and Authentication (Organizational Users)	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)	Identification and Authentication (Organizational Users)	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)	Incident Handling	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions.
MA-4 (6)	Non-Local Maintenance	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.
MA-5 (1)	Maintenance Personnel	The organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: a. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; b. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and c. In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.
MP-2 (2)	Media Access	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-6 (3)	Media Sanitization	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 (5)	Media Sanitization	The organization sanitizes information system media containing classified information in accordance with NSA standards and policies. (Inconsistent: Technically the only classified information is at impact level 6, and this control should not apply to the others, contrary to what has been identified in the draft

		requirements.)
MP-6 (6)	Media Sanitization	The organization destroys information system media that cannot be sanitized.
PE-3 (2)	Physical Access Control	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)	Physical Access Control	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)	Access Agreements	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)	Vulnerability Scanning	The organization attempts to discern what information about the information system is discoverable by adversaries.
RA-5 (5)	Vulnerability Scanning	The organization includes privileged access authorization to *operating systems/infrastructure, databases, web applications* for selected vulnerability scanning activities to facilitate more thorough scanning.
SA-12 (2)	Supply Chain Protection	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)	Transmission Confidentiality	The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-13 (4)	Use of Cryptography	The organization employs the following cryptography to implement digital signatures: • *NIST FIPS-Validated for Unclassified systems (Impact levels 2-5)* • *NSA Approved/FIPS-Validated for Classified systems (Impact level 6)*
SC-18 (2)	Mobile Code	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets organization defined mobile code requirements. • *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 ECSB DAA.*
SC-23 (1)	Session Authenticity	The information system invalidates session identifiers upon user logout or other session termination.
SC-23 (2)	Session Authenticity	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.
SC-23 (3)	Session Authenticity	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.
SC-23 (4)	Session Authenticity	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)	Information System Monitoring	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
SI-4 (7)	Information System Monitoring	The information system notifies *organization defined incident response personnel (by name and/or 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)	Information System Monitoring	The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-4 (9)	Information System Monitoring	The organization tests/exercises intrusion-monitoring tools *weekly*.

5.2.3 CNSSI 1253 Additional Control Set 2

CNSSI Additional Control Set 2			
Impact	**IaaS**	**PaaS**	**SaaS**
3			✓
4			✓
5			✓

Additional Control Set 2		
ID	**Control Name**	**Description**
AC-3 (4)	Access Enforcement	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.
CM-4 (1)	Security Impact Analysis	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.
SI-8 (1)	SPAM Protection	The organization centrally manages spam protection mechanisms.
SI-8 (2)	SPAM Protection	The information system automatically updates spam protection mechanisms (including signature definitions).

5.2.4 CNSSI 1253 Additional Control Set 3

CNSSI Additional Control Set 3			
Impact	**IaaS**	**PaaS**	**SaaS**
3			✓
4			✓
5	✓	✓	✓

Additional Control Set 3		
ID	**Control Name**	**Description**
IA-5 (4)	Authenticator Management	The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.

5.2.5 CNSSI 1253 Additional Control Set 4

CNSSI Additional Control Set 4			
Impact	**IaaS**	**PaaS**	**SaaS**
5	✓	✓	✓

Control Set 4		
ID	**Control Name**	**Description**
AC-3 (6)	Access Enforcement	The organization encrypts or stores off-line in a secure location *Sensitive, Controlled Unclassified Information (CUI) and classified non-SAMI information*.
AC-6 (6)	Least Privilege	The organization prohibits privileged access to the information system by non-organizational users.
AC-7 (1)	Unsuccessful Login Attempts	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
AC-9	Previous Logon	The information system notifies the user, upon successful logon (access), of the date and time of

	(Access) Notification	the last logon (access).
AC-17 (6)	Remote Access	The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
AU-5 (1)	Response to Audit Processing Failures	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)	Response to Audit Processing Failures	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* • *audit storage capacity being reached or exceeded*
AU-9 (3)	Protection of Audit Information	The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.
AU-9 (4)	Protection of Audit Information	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.
AU-12 (1)	Audit Generation	The information system compiles audit records from *all information systems 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)	Security Assessments	The organization includes as part of security control assessments, *annually or more frequent 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*.
CM-2 (2)	Baseline Configuration	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
CM-3 (1)	Configuration Change Control	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 *7 days or as negotiated in the SLA*; d. Inhibit change until designated approvals are received; and e. Document completed changes to the information system.
CM-3 (4)	Configuration Change Control	The organization requires an information security representative to be a member of the *Configuration Control Board*.
CM-5 (2)	Access Restrictions for Change	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)	Access Restrictions for Change	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-6 (2)	Configuration Settings	The organization employs automated mechanisms to respond to unauthorized changes to *security related configuration settings defined at the program/system level*.
CM-8 (2)	Information System Component Inventory	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.
CM-8 (4)	Information System Component Inventory	The organization includes in property accountability information for information system components, a means for identifying by [Selection (one or more): name; position; role] individuals responsible for administering those components.
IA-2 (4)	Identification and Authentication (Organizational	The information system uses multifactor authentication for local access to non-privileged accounts.

	Users)	
IA-3 (1)	Device Identification and Authentication	The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.
IA-3 (2)	Device Identification and Authentication	The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.
IA-3 (3)	Device Identification and Authentication	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.
IR-2 (1)	Incident Response Training	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
IR-6 (2)	Incident Reporting	The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
MA-4 (3)	Non-Local Maintenance	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 (5)	Non-Local Maintenance	The organization requires that: a. Maintenance personnel notify [Assignment: organization-defined personnel] when non-local maintenance is planned (i.e., date/time); and b. A designated organizational official with specific information security/information system knowledge approves the non-local maintenance.
MA-4 (7)	Non-Local Maintenance	The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.
MP-6 (1)	Media Sanitization	The organization tracks, documents, and verifies media sanitization and disposal actions.
MP-6 (2)	Media Sanitization	The organization tests sanitization equipment and procedures to verify correct performance [Assignment: organization-defined frequency].
PE-3 (1)	Physical Access Control	The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility
PE-3 (4)	Physical Access Control	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)	Physical Access Control	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)	Access Records	The organization maintains a record of all physical access, both visitor and authorized individuals.
SA-5 (4)	Information System Documentation	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)	Developer Security Testing	The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.
SC-3	Security Function Isolation	The information system isolates security functions from non-security functions.

SC-7 (11)	Boundary Protection	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)	Transmission Integrity	The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.
SC-24	Fail In Known State	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*.
SC-28 (1)	Protection of Information at Rest	The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.
SC-33	Transmission Preparation Integrity	The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.
SI-7 (2)	Software and Information Integrity	The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

5.3 C2 and NetOps Requirements

5.3.1 C2 and NetOps Baseline Requirements

C2 Baseline Requirements			
Impact	**IaaS**	**PaaS**	**SaaS**
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓

ID	Requirement	Description
C2-1	Incident Reporting	Providers are required to submit incident reports to FedRAMP and the provider's container (DISA or other DoD cloud customer) for the following incident categories: • 1. Root Level Intrusion • 2. User Level Intrusion • 4. Denial of Service • 5. Non-Compliance Activity • 7. Malicious Logic
C2-2	Communication with CND Tier II	The provider can communicate unclassified information to CND Tier II: • DIBNet-U • Encrypted VPNs • Encrypted web connections • Encrypted email • Secure Phone
C2-3	Vulnerability Scans	Results of periodic vulnerability scans of cloud provider systems must be reported to CND Tier II in CSV or XML format. • CND Tier II will provide assistance and corrective actions
C2-4	Plan of Action and Milestones	All providers must send current version of the POA&M (required by FedRAMP) to CND Tier II.
C2-5	Warnings and Notifications	CSPs must receive, act upon, and report compliance with warnings and notifications from Tier I or II CND.
C2-6	Network Architecture and Security Package Documentation	Providers must supply network architecture documentation and the FedRAMP security package to Tier II CND. • The information must be no older than 6 months.
C2-7	Network Security Configuration Changes	CND Tier II must be notified of any planned changes to network security configurations. • Change management documentation can be provided to satisfy this requirement.
C2-8	Scheduled Outages	Tier II CND must be notified of all planned system outages in advance and of all activities planned during the outage.

5.3.2 C2 and NetOps Additional Requirements Set 1

The requirements identified in the table below are designed to replace those outlined in 5.1.

C2 Additional Requirements Set 1			
Impact	**IaaS**	**PaaS**	**SaaS**
4	✓	✓	✓
5	✓	✓	✓

ID	Requirement	Description
C2-1	Incident Reporting	Providers are required to submit incident reports to FedRAMP and the provider's container (DISA or other DoD cloud customer) for the following incident categories: • 1. Root Level Intrusion • 2. User Level Intrusion • 3. Unsuccessful Activity Attempt • 4. Denial of Service • 5. Non-Compliance Activity • 7. Malicious Logic
C2-2	Communication with CND Tier II	The provider can communicate to CND Tier II: a. Unclassified information via: • Encrypted VPNs • Encrypted web connections • DoD PKI encrypted email • Secure Phone b. Classified information via: • DIBNet-S

5.3.3 C2 and NetOps Additional Requirements Set 2

The requirements identified in the table below replace any duplicates those outlined in 5.3.1 and 5.3.2.

C2 Additional Requirements Set 2			
Impact	IaaS	PaaS	SaaS
5		✓	✓

ID	Requirement	Description
C2-2	Communication with CND Tier II	The provider can communicate to CND Tier II: a. Unclassified information via: • DIBNet-U • Encrypted VPNs • Encrypted web connections • encrypted email • Secure Phone b. Classified information via: • DIBNet-S

5.4 Architecture Integration Requirements

AI Baseline Requirements

5.4.1 AI Baseline Requirements

Impact	IaaS	PaaS	SaaS
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓

ID	Requirement	Description
AI-1	Host Based Security	CSPs must permit and not interfere with the installation of the Host Based Security System (HBSS) and secure communication between HBSS components and any secure communication required between those components and HBSS components hosted outside the CSP boundary.
AI-2	DoD PKI	CSPs must provide either multi-factor one-time password or PKI certificate technology authentication for administrative access.
AI-2 (1)	DoD PKI	Whenever a CSP is responsible for authentication of entities and/or identifying a hosted DoD information system, the CSP shall 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.
AI-2 (2)	DoD PKI	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.
AI-2 (3)	DoD PKI	DoD issued PKI certificates shall be used to identify applications and service contracted for by the DoD.
AI-2 (4)	DoD PKI	CSP personnel and CSP owned assets may use DoD ECA issued PKI certificates for identification, or DoD issued PKI certificates when available.
AI-3	Secure Communications and Collaboration Environment	CSPs 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. a. Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet.
AI-4	Separation of DoD Data	CSP systems that contain DoD data shall have no external connections other than those authorized by DISA. a. All authorized external connections from CSP systems shall be to the NIPRNET.
AI-4 (1)	Separation of DoD Data	CSP systems that contain DoD data must provide appropriate separation to ensure that any inter-connectivity between CSP resources ensures adequate security: a. The DoD resources must be physically separated, or logically separated to a sufficient degree of assurance, from any non-DoD resources. b. The CSP implementation will ensure a clear, manageable boundary between the DoD content and the non-DoD content. c. The CSP logical separation must ensure appropriate security to the DoD customer data content.
AI-5	Separation of DoD Data	CSP systems that are multi-tenant with both DoD and non-DoD customers have to meet additional controls for logical separation of DoD data in-transit, in-process, and at-rest: a. Data in transit and at-rest must be cryptographically separated from non-DoD data using FIPS-140 validated cryptographic modules. b. Key management modules must also be FIPS-140 compliant and implemented in a way that assures keys cannot be accessed by non-DoD tenants. c. Active virtual machines shall be restricted by mandatory access controls to protect data in-process from other tenants. d. CSPs shall use hypervisors that support trusted execution, hardware-assisted virtualization, and I/O virtualization CPU instruction sets, and must be run on hardware that is compatible with such instruction sets. e. NIPRNet connections to CSP systems shall be implemented through network interface cards that are dedicated exclusively to DoD tenants by the hypervisor, utilizing I/O virtualization CPU instructions for assurance that non-DoD tenants cannot access them.

AI Additional Requirements Set 1

5.4.2 AI Additional Requirements Set 1

Impact	IaaS	PaaS	SaaS
4	✓		
5	✓		

ID	Requirement	Description
AI-3	Secure Communications and Collaboration Environment	CSPs operating at 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. a. Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet.

5.4.3 AI Additional Requirements Set 2

AI Additional Requirements Set 2			
Impact	**IaaS**	**PaaS**	**SaaS**
4		✓	✓
5		✓	✓

ID	Requirement	Description
AI-3	Secure Communications and Collaboration Environment	CSPs operating at 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. a. Secure communications and collaboration between a CSP and the DoD will occur primarily via DIBNet.

5.5 Policy, Guidance, and Operational Constraints Requirements

5.5.1 PGO Baseline Requirements

The following requirements are impact levels and cloud architectures (IaaS, PaaS, or SaaS).

PGO Baseline Requirements			
Impact	**IaaS**	**PaaS**	**SaaS**
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓

ID	Requirement	Description
PGO-1 (1)	STIGs and SRGs	The providers will address and document the intent of the STIGs or SRGs for technologies without a STIG or SRG.
PGO-2	Law Enforcement Access	A CSP will provide any request for data including meta data and web matrix monitoring for law enforcement purposes within 3 days, however if the request for data involves risk to property, loss of life, or a national security/criminal threat the CSP will provide the information within 24 hours if not sooner.
PGO-2 (1)	Law Enforcement Access	A CSP shall afford federal law enforcement agents, including but not limited to agents of the U.S. Department of Justice, the Offices of the Inspector Generals, and the U.S. Department of Homeland Security, at all times and without prior written notice, access to the Data Center and Data, as well as to make copies or extracts therefrom, if the federal law enforcement agency certifies that such urgency exists. • To any and all extent possible, a CSP shall segregate the data and afford access to

		such information in a secure and private space, and without CSP presence, if requested.
PGO-2 (2)	Law Enforcement Access	The CSP will log all access to the government data. a. 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, • other data as the government may specify from time to time. b. 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 entity immediately upon request.
PGO-2 (3)	Law Enforcement Access	Unless otherwise exempt from doing the same by law, the CSP must provide all federal law enforcement 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.
PGO-2 (4)	Law Enforcement Access	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 law enforcement officials.
PGO-3	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 would impact any server that stores US Government Data. • A CSP will cooperate with the agency and the US Department of Justice to take all measures to protect the sovereignty of US Government data from any court, foreign, state, or local government or other legal proceeding.
PGO-3 (1)	Notification	The CSP shall not report or provide breach notification under State law or otherwise, unless the CSP has provided the Agency with prior timely notice, so that the Agency may coordinate, intervene, or otherwise assert or protect its legal and procedural rights with respect to such reporting or notification
PGO-4	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.
PGO-4 (1)	Personnel Access	All employees of the CSP who have access to government data must sign a non-disclosure form.
PGO-5	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.
PGO-5 (1)	Continuous Monitoring	If requested by the customer agency, the CSP will provide any additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements within 10 business days.
PGO-6	Privacy Impact Assessments	If the cloud service entails operation or maintenance of a Privacy Act System of Records the following apply: • FAR Section 352.224-70: Privacy Act • FAR Section 52.239-1: Privacy or Security Safeguards • Privacy Impact Assessments
PGO-6 (1)	Privacy Impact Assessments	The provider must report to the agency information as required for completion of a Privacy Impact Assessment (PIA) for information technology that is developed or procured to collect, maintain, or disseminate information in identifiable form and for certain other electronic information activities that would permit the physical or online contacting of an individual.
PGO-6 (2)	Privacy Impact Assessments	The privacy impact assessment will be provided to the specified Agency designee no later than (date or number of calendar days) with the following information: a. What information is to be collected (e.g., nature and source); b. Why the information is being collected (e.g., to determine eligibility); c. Intended use of the information (e.g., to verify existing data); d. With whom the information will be shared (e.g., another agency for a specified

		programmatic purpose); e. What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent; f. How the information will be secured (e.g., administrative and technological controls); and g. Whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. In the absence of a designated Agency designee for the PIA report, the CSP shall ensure that all information required within this clause is available and that a report providing the information can be produced within 10 days of formal request from either the Contracting Officer or the Contracting Officer's Representative. The agency may require and direct that the CSP, in lieu of the Agency, conduct and prepare the PIA as part of the design or development process.
PGO-6 (3)	Privacy Impact Assessments	The CSP will also collaborate with the Agency to revise the PIA should a change to the system result in a significant way in which PII is collected or maintained within the system.
PGO-7	Data Locations	A CSP will maintain all US Government data on this contract within the States, districts, and territories 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.
PGO-8	Data Spills	If a data spill is discovered by a CSP, the CSP shall: • Report the incident in accordance with incident reporting guidelines • Take reasonable steps to contain data contamination • Take reasonable steps to identify scope of contamination, including all systems, networks, and storage hardware that are affected • Await response instructions from DoD before taking further action.
PGO-9	Disposition of Data	Upon request by 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. a. DoD cloud customer may also request different means of data transfer (for example, as called out in the SLA), at its discretion.
PGO-9 (1)	Disposition of Data	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. a. Alternatively, CSP may provide some equivalent assurance of data destruction, at the discretion of DoD cloud customer.
PGO-10	Disposal of Storage Hardware	CSP shall: a. Purge all data on devices prior to disposal, reuse, or transfer in accordance with NIST 800-88 b. Physically destroy devices that are unable to be cleared or purged, as defined in NIST 800-88. c. Destroy any devices, in accordance with NIST 800-88, when there is any doubt to the success of the cleared or purged process.

5.5.2 PGO Additional Requirements Set 1

PGO Additional Requirements Set 1			
Impact	**IaaS**	**PaaS**	**SaaS**
3	✓		
4	✓		
5	✓		

ID	Requirement	Description
PGO-1	Security Technical Implementation Guides (STIGs)	The provider will address and document conformity with the Security Technical Implementation Guides (STIGs): a. NIST SP 800-125 "Guide to Security for Full Virtualization Technologies" b. ESX Server STIG Version 1, Release 1 c. VMWare ESXi v5 STIG DRAFT, Version 1 (currently in draft status)

		STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses.

5.5.3 PGO Additional Requirements Set 2

PGO Additional Requirements Set 2			
Impact	**IaaS**	**PaaS**	**SaaS**
3		✓	
4		✓	
5		✓	

ID	Requirement	Description
PGO-1	Security Technical Implementation Guides	The provider will address and document conformity with the Security Technical Implementation Guides (STIGs): a. Domain Name Service STIG b. Operating System • Windows STIGs • Unix SRG & STIGs • Apple OS X STIG • zOS STIG • SUSE Linux Enterprise System V11 STIG c. Remote Computing • Thin Client Server (SunRay STIG) • Citrix XenApp Server STIGs d. Other Related STIGs • ESX Server STIG Version 1, Release 1 • VMWare ESXi v5 STIG DRAFT, Version 1 (currently in draft status) • HMC STIG • Google Chrome STIG e. Other • NIST SP 800-125 “Guide to Security for Full Virtualization Technologies” STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses.

5.5.4 PGO Additional Requirements Set 3

PGO Additional Requirements Set 3			
Impact	**IaaS**	**PaaS**	**SaaS**
3			✓
4			✓
5			✓

ID	Requirement	Description
PGO-1	Security Technical Implementation Guides	The provider will address and document conformity with the Security Technical Implementation Guides (STIGs): a. 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 • Web Browser STIGs • Microsoft Exchange STIGs • Microsoft SharePoint 2010 STIG • Google Chrome STIG b. Domain Name Service STIG c. Operating System • Windows STIGs • Unix SRG & STIGs • Apple OS X STIG • zOS STIG • SUSE Linux Enterprise System V11 STIG d. Remote Computing • Thin Client Server (SunRay STIG) • Citrix XenApp Server STIGs • Thin Client Server (SunRay STIG) • Citrix XenApp Server STIGs e. Web/App/DB Server • Web Server SRG(s)/STIG(s) • Application Server SRG(s)/STIG(s) • Database SRG(s)/STIG(s) • .NET SRG(s) STIG(s) • JRE SRG(s)/STIG(s) f. Other Related STIGs • ESX Server STIG Version 1, Release 1 • VMWare ESXi v5 STIG DRAFT, Version 1 (currently in draft status) • HMC STIG • Instant Messaging STIG • VVoIP STIG • VTC STIG • Enterprise Resource Planning (ERP) STIG • Enterprise System Management (ESM) STIG g. Other • NIST SP 800-125 "Guide to Security for Full Virtualization Technologies" STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses.

5.6 Assessment of FedRAMP Plus DISA Requirements

Our research successfully consolidates cloud requirements from multiple, disparate sources. It offers a single reference that contains the available information needed to transition from private to public, DoD cloud services. This resource will save hundreds of hours each provider must expend to identify requirements. Further, it will assist cloud providers and government users in determine the suitability of a cloud architecture to their needs and DoD requirements.

5.6.1 Inconsistencies and Potential Errors

Our research identified several potential errors in the current requirements. These include:

- In section 6.2 C2-2, the DIBNet-U option is not allowed for impact level 4 (IaaS, PaaS, SaaS) or impact level 5 (IaaS), but is accepted in section 6.3 C2-2 for the higher, impact level 5 (PaaS, SaaS).

- In section 6.2 and 6.3, C2-2 specifies that classified information is to be sent using DIBNet-S, yet it is unclear why any classified information would exist for any of these systems, which exist at impact levels 3, 4, 5; which are Unclassified Private (Impact Level 3) and Unclassified Controlled (Impact Levels 4 and 5).

- In section 6.2, C2-2, impact level 4 (IaaS, PaaS, SaaS) and level 5 (IaaS) requires transmission of unclassified information through DoD PKI encrypted email. This requirement disappears in section 6.3 for the higher impact level 5 systems (PaaS, SaaS), only requiring encrypted email.

- In section 7.2, AI-3, users are required to use DIBNet-S for transmission of sensitive information for Impact Level 4 and 5 IaaS. For AI-3 in section 7.3 DISA requires use of DIBNet-U for sensitive data for Impact Level 4 and 5 PaaS/SaaS. This appears to be inconsistent and both should most likely be DIBNet-U or DIBNet-S.

- In the DISA documentation [59], the document editor cut & pasted the wrong material multiple times (see page E-23 for Level 5 "CSPs operating at Level 3 are required…").

- Several of the fields for added CNSSI 1251 controls were left undefined (e.g., CM-8 (4), MA-4 (5), MP-6 (2)).

- In Section 8.4, PGO-1, the implementation guides are duplicated under section "d. Remote Computing".

- In Section 8.1, PGO-6 (3), the guidance states that "the agency may require and direct that the CSP, in lieu of the Agency, conduct and prepare the privacy impact assessment (PIA) as part of the design or development process". The language suggests that the DoD anticipates a custom design or development process for each deployment. This is unlikely to be feasible for most cloud providers.

Instances exist where, potentially due to errors in draft requirements, FedRAMP Plus controls were actually less stringent than the base FedRAMP controls. One example of this is in section 5.1.5 control AC-10, where FedRAMP limits the number of concurrent sessions for each system account to one session, but DISA indicates three are allowable for privileged access and two for non-privileged access. Since FedRAMP certification is a basic requirement for DISA certification, and in these instances FedRAMP requires are more stringent, it can be assumed that the DISA restrictions are void. In these instances, the cloud provider must address the most stringent requirement for both FedRAMP and agency specific certifications. We suggest identifying all requirements, both FedRAMP and agency specific, prior to implementing controls. If a provider attempted to implement requirements independently, they may inadvertently violate FedRAMP requirements while implementing those of another certifying body.

6 References

[1] http://talkincloud.com/tc100

[2] http://www.businessinsider.com/10-most-important-in-cloud-computing-2013-4#no-8-citrix-systems-is-taking-on-vmware-with-some-success-4

[3] http://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php

[4] http://research.microsoft.com/en-us/um/people/pcosta/slides/costa12naas_slides.pdf

[5] Citrix, "Products for Virtualization, Networking, and Cloud Computing Solutions", http://www.citrix.com/products.html

[6] GoToMeeting, "GoToMeeting Pricing | GoToMeeting", http://www.gotomeeting.com/online/meeting/pricing?c_name=ctxs&c_prod=GTM&c_cmp=sf-70150000000ZS3c

[7] Microsoft Office 365, "What is Office 365 for business?" http://office.microsoft.com/en-us/business/what-is-office-365-for-business-FX102997580.aspx

[8] Google Apps, "Pricing", http://www.google.com/enterprise/apps/business/pricing.html

[9] Salesforce.com, "Salesforce Pricing & Editions – Service Cloud – Salesforce.com", http://www.salesforce.com/crm/editions-pricing-service.jsp?d=70130000000rz42&internal=true

[10] Cisco WebEx Cloud, "Cisco WebEx Cloud Collaboration – Cisco Systems", http://www.cisco.com/en/US/solutions/ns1007/ns1234/collaboration_cloud.html

[11] Cisco WebEx, "WebEx Meeting Plans: Free, Premium, Premium Plus, and Enterprise", http://www.webex.com/plans/meetings-plans.html

[12] McAfee, "McAfee Security-as-a-Service | McAfee Products", http://www.mcafee.com/us/products/security-as-a-service/index.aspx/

[13] DropBox, "Dropbox – Pricing – Dropbox for Business" , https://www.dropbox.com/business/pricing

[14] LogMeIn, "LogMeIn – Buy LogMeIn Pro Today", https://secure.logmein.com/products/pro/purchase.aspx

[15] Trend Micro SecureCloud, "SecureCloud – Virtual Cloud Security – Trend Micro USA", http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_securecloud.pdf

[16] Trend Micro, "Cloud and Data Center Security" – Trend Micro USA", http://www.trendmicro.com/us/business/cloud-data/index.html

[17] Trend Micro, "Virtualization Security Technology – Data Center Virtualization – Deep Security – Trend Micro USA", http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/index.html

[18] Intermedia, “Office in the Cloud Services”, http://www.intermedia.net/solutions/office-in-the-cloud#services

[19] Intermedia, “Compare our Bundles”, http://www.intermedia.net/solutions/office-in-the-cloud#compare

[20] ConnectWise, “ConnectWise Overview”, http://www.connectwise.com/connectwise-overview.php

[21] Symantec, “Symantec Email Security.cloud”, http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-symantec-email-security-cloud_DS.en-us.pdf

[22] Amazon AWS, “Amazon EC2 Pricing”, http://aws.amazon.com/ec2/pricing/

[23] Amazon AWS, “Amazon AWS Support Pricing”, https://aws.amazon.com/premiumsupport/pricing/

[24] Windows Azure, “Solutions”, http://www.windowsazure.com/en-us/solutions/

[25] Windows Azure, “Purchase Options”, http://www.windowsazure.com/en-us/pricing/purchase-options/

[26] Windows Azure, “Windows Azure Support Plans”, http://www.windowsazure.com/en-us/support/plans/

[27] Salesforce Force.com, “Force.com Product Comparison”, http://www.sfdcstatic.com/assets/pdf/datasheets/DS_Forcedotcom_EdCompare.pdf

[28] Google App Engine, “Google App Engine Pricing”, https://cloud.google.com/pricing/

[29] Rackspace, “Pricing”, http://www.rackspace.com/cloud/servers/pricing/

[30] Rackspace, “Support”, http://www.rackspace.com/knowledge_center/product-faq/cloud-servers

[31] ThinkGrid, “Support”, http://www.thinkgrid.com/about-us/support/

[32] FindTheBest, “Terremark vs. ThinkGrid”, http://cloud-computing.findthebest.com/compare/22-121/Terremark-vs-ThinkGrid

[33] OpenShift, “Enterprise Platform as a Service”, https://www.openshift.com/products/enterprise

[34] OpenShift, “OpenShift Online Pricing”, https://www.openshift.com/products/pricing

[35] RightScale, “Why RightScale”, http://www.rightscale.com/products/why-rightscale.php

[36] RightScale, “RightScale Pricing”, http://www.rightscale.com/products/plans-pricing/

[37] Google Compute Engine, “Google Compute Engine”, https://cloud.google.com/products/compute-engine

[38] Google Compute Engine, “Google Compute Engine Pricing”, https://cloud.google.com/pricing/compute-engine

[39] HP Cloud, “HP Cloud Pricing”, http://www.hpcloud.com/pricing

[40] HP Cloud, “HP Public Cloud Support”, http://www.hpcloud.com/content/hp-cloud-services-support

[41] OpenStack, “OpenStack Open Source Cloud Computing Softwware”, http://www.openstack.org/

[42] Verizon Terremark, “Verizon Cloud”, http://www.terremark.com/verizoncloud

[43] FindTheBest, “Savvis vs. Terremark”, http://cloud-computing.findthebest.com/compare/21-22/Savvis-vs-Terremark

[44] Verizon Terremark, “Terremark Boosts Support Levels, Unveils New Pricing Models for vCloud Express Service”, http://www.terremark.com/about/news-events/news/2011/04072011.aspx

[45] IBM SmartCloud Enterprise, “IBM Infrastructure as a Service”, http://www-935.ibm.com/services/us/en/cloud-enterprise/

[46] IBM SmartCloud Enterprise, “IBM SmartCloud Enterprise – Agreements and Disclosure”, http://www-935.ibm.com/services/us/en/cloud-enterprise/contracts/ibm_productimages.html

[47] IBM SmartCloud Enterprise, “IMB SmartCloudEnterprise – Charges Schedule”, http://www-935.ibm.com/services/us/en/cloud-enterprise/contracts/charges_schedule.html

[48] IBM SmartCloud Enterprise, “IBM SmartCloud Enterprise – Support”, https://www-147.ibm.com/cloud/enterprise/support

[49] SoftLayer CloudLayer, “CloudLayer Computing”, http://www.softlayer.com/cloudlayer/computing/

[50] Savvis, “Cloud Data Center”, http://www.savvis.com/cloud/data-center

[51] SavvisDirect, “Cloud Server Pricing”, https://www.savvisdirect.com/cloud-servers/pricing

[52] SavvisDirect, “Premium Support Services for Virtual Infrastructure”, http://www.savvisdirect.com/cloud-support-iaas

[53] Artisan Infrastructure, “Home”, http://www.artisaninfrastructure.com/Pages/default.aspx

[54] Artisan Infrastructure, “PressNews – Artisan Infrastructure Introduces First Wholesale Only Object Based Cloud Storage Platform”, http://www.artisaninfrastructure.com/Lists/PressNews/DisplayPressNews.aspx?ID=24

[55] Aryaka, “Network as-a-Service”, http://www.aryaka.com/products/network-as-a-service/

[56] Aerohive Networks, “Network-as-a-Service (NaaS) Subscription, http://www.aerohive.com/products/cloud-services-platform/network-service-naas-subscription

[57] Pertino, “Pricing”, http://pertino.com/pricing

[58] OpenNaaS, “Overview”, http://www.opennaas.org/

[59] DISA, “Cloud Security Model Version 2.0 Draft Master”

[60] DISA, “Cloud Security Model Control Parameters Annex Version 1.1” http://iase.disa.mil/cloud_security/downloads/DoD%20Enterprise%20Cloud%20Service%20Broker%20Cloud%20Security%20Model%20Control%20Parameters%20Annex%20Version%201.1%2020131324.pdf

[61] FedRAMP, “Federal Risk and Authorization Management Program (FedRAMP) Security Controls”

[62] FedRAMP, “FedRAMP_Baseline_Security_Controls_v1.0”

[63] NIST, “NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations” http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[64] Sandia, “CNSSI Instruction No. 1253”, http://www.sandia.gov/FSO/PDF/flowdown/Final_CNSSI_1253.pdf

[65] FedRAMP, “FedRAMP Security Assessment”, http://www.gsa.gov/portal/category/102999

[66] FedRAMP, “FedRAMP Processes”, http://www.gsa.gov/portal/category/102995

[67] FedRAMP, “Ongoing Assessment & Authorization”, http://www.gsa.gov/portal/category/103155

[68] NIST, “NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf