

Chapter One: Cloud Computing Security Requirements Baseline

1. Cloud Computing Security Requirements Baseline

This chapter identifies (by security control number and name) the security controls from NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (as amended). These controls have been agreed to by a Joint Approval Board made up of users from GSA, DHS & DOD for use within information systems providing cloud computing services to the Federal government.

The security controls contained in this publication work in concert with NIST Special Publication 800-53, Revision 3. Table 1 (begins on page 3) specifies control parameter definitions and additional requirements or guidance in addition to NIST Special Publication 800-53, Revision 3 for a FedRAMP A&A package. NIST Special Publication 800-53, Revision 3 details security controls that apply to all federal information systems, and authorizing officials and information system owners have the authority and responsibility to develop security plans which define how the controls are implemented within their particular information systems and environments of operation.

In the case of FedRAMP, two sets of security controls have been defined for low-impact and moderate-impact cloud information systems respectively. The impact levels are based on the sensitivity and criticality of the federal information being processed, stored, and transmitted by cloud information systems as defined in Federal Information Processing Standard 199. All NIST security standards and guidelines used to define the requirements for the FedRAMP cloud computing initiative are publicly available at <http://csrc.nist.gov>.

The FedRAMP defined security controls are presented in Table 1: FedRAMP Security Controls. This table is organized by the 17 control families identified in NIST Special Publication 800-53, Revision 3. The table presents the following information:

- **Control Number and Name** – The control number and control name relate to the control as defined in NIST Special Publication 800-53, Revision 3.
- **Control Baseline** – The control is listed in either the Low or Moderate impact column where applicable to that baseline. If the control is not applicable, a blank will appear in that column. If a control enhancement is applicable, the enhancement is designated inside of parenthesis. Additional security controls and control enhancements that are not included in the low and moderate control baselines defined in NIST Special Publication 800-53 Revision 3 (Appendix D) are denoted in **bold** font. For example,
AC-2 : Control is included in the NIST Baseline
AC-2 (1) : Control enhancement is included in the NIST Baseline
AC-2 (7) : FedRAMP specific control enhancement.
- **Control Parameter Requirements** – Certain controls are defined with implementation parameters. These parameters identify the scope, frequency and other considerations for how cloud service providers address specific controls and enhancements.
- **Additional Requirements & Guidance** – These entries represent additional required security controls for cloud computing applications and environments of operation selected from the security control catalog in NIST Special Publication 800-53 Revision 3 (Appendix F). Required parameter *values* for the variable parts of security controls and control enhancements (designated by *assignment* and *selection* statements) are also provided.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
1.1. Access Control (AC)					
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AC-2	Account Management	AC-2	AC-2 AC-2 (1) AC-2 (2) AC-2 (3) AC-2 (4) AC-2 (7)	AC-2]. [Assignment: organization-defined frequency] Parameter: [at least annually] AC-2 (2) [Assignment: organization-defined time period for each type of account (temporary and emergency)] Parameter: [no more than ninety days for temporary and emergency account types] AC-2 (3) [Assignment: organization-defined time period] Parameter: [ninety days for user accounts] See additional requirements and guidance.	AC-2 (3) Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB.
AC-3	Access Enforcement	AC-3	AC-3 AC-3 (3)	AC-3 (3) [Assignment: organization-defined nondiscretionary access control policies] Parameter: [role-based access control] [Assignment: organization-defined set of users and resources] Parameter: [all users and resources]	AC-3 (3) Requirement: The service provider: a. Assigns user accounts and authenticators in accordance within service provider's role-based access control policies; b. Configures the information system to request user ID and authenticator prior to system access; and c. 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	Not Selected	AC-4	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AC-5	Separation of Duties	Not Selected	AC-5	None.	None.
AC-6	Least Privilege	Not Selected	AC-6 AC-6 (1) AC-6 (2)	<p>AC-6 (1) [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware and security-relevant information)] Parameter: See additional requirements and guidance.</p> <p>AC-6 (2) [Assignment: organization-defined list of security functions or security-relevant information] Parameter: [all security functions]</p>	<p>AC-6 (1) Requirement: The service provider defines the list of security functions. The list of functions is approved and accepted by the JAB.</p> <p>AC-6 (2) Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.</p>
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	<p>AC-7a. [Assignment: organization-defined number] Parameter: [not more than three]</p> <p>AC-7a. [Assignment: organization-defined time period] Parameter: [fifteen minutes]</p> <p>AC-7b. [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] Parameter: [locks the account/node for thirty minutes]</p>	None.
AC-8	System Use Notification	AC-8	AC-8	None.	None.
AC-10	Concurrent Session Control	Not Selected	AC-10	<p>AC-10 [Assignment: organization-defined number] Parameter: [one session]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AC-11	Session Lock	Not Selected	AC-11 AC-11 (1)	AC-11a. [Assignment: organization-defined time period] Parameter: [fifteen minutes]	None.
AC-14	Permitted Actions Without Identification/ Authentication	AC-14	AC-14 AC-14 (1)	None.	None.
AC-16	Security Attributes	Not Selected	AC-16	AC-16 Assignment: organization-defined security attributes] Parameter: See additional requirements and guidance.	AC-16 Requirement: The service provider defines the security attributes. The security attributes need to be approved and accepted by JAB.
AC-17	Remote Access	AC-17	AC-17 AC-17 (1) AC-17 (2) AC-17 (3) AC-17 (4) AC-17 (5) AC-17 (7) AC-17 (8)	AC-17 (5) [Assignment: organization-defined frequency] Parameter: [continuously, real time] AC-17 (7) [Assignment: organization-defined list of security functions and security-relevant information] Parameter: See additional requirements and guidance. AC-17 (8) [Assignment: organization-defined networking protocols within the information system deemed to be non-secure] Parameter: [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]	AC-17 (7) Requirement: The service provider defines the list of security functions and security relevant information. Security functions and the implementation of such functions are approved and accepted by the JAB. Guidance: Security functions include but are not limited to: establishing system accounts; configuring access authorizations; performing system administration functions; and auditing system events or accessing event logs; SSH, and VPN. AC-17 (8) Requirement: Networking protocols implemented by the service provider are approved and accepted by JAB. Guidance: Exceptions to restricted networking protocols are granted for explicitly identified information system components in support of specific operational requirements.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AC-18	Wireless Access	AC-18	AC-18 AC-18 (1) AC-18 (2) AC-18 (3) AC-18 (4) AC-18 (5)	AC-18 (2) [Assignment: organization-defined frequency] Parameter: [at least quarterly]	None.
AC-19	Access Control for Mobile Devices	AC-19	AC-19 AC-19 (1) AC-19 (2) AC-19 (3)	AC-19g. [Assignment: organization-defined inspection and preventative measures] Parameter: See additional requirements and guidance.	AC-19g. Requirement: The service provider defines inspection and preventative measures. The measures are approved and accepted by JAB.
AC-20	Use of External Information Systems	AC-20	AC-20 AC-20 (1) AC-20 (2)	None.	None.
AC-21	User-Based Collaboration and Information Sharing	Not Selected	AC-21	AC-21a. [Assignment: organization-defined information sharing circumstances where user discretion is required] Parameter: See additional requirements and guidance. AC-21b. [Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required] Parameter: See additional requirements and guidance.	AC-21a. Requirement: The service consumer defines information sharing circumstances where user discretion is required. AC-21b. Requirement: The service provider defines the mechanisms or manual processes for the information sharing circumstances defined by the service consumer.
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22d. [Assignment: organization-defined frequency] Parameter: [at least quarterly]	None.
1.2. Awareness and Training (AT)					
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AT-2	Security Awareness	AT-2	AT-2	AT-2 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AT-3	Security Training	AT-3	AT-3	AT-3 [Assignment: organization-defined frequency] Parameter: [at least every three years]	None.
AT-4	Security Training Records	AT-4	AT-4	AT-4b. [Assignment: organization-defined frequency] Parameter: [At least three years]	None.
AT-5	Contacts With Security Groups and Associations	Not Selected	AT-5	None	None.
1.3. Audit and Accountability (AU)					
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AU-2	Auditable Events	AU-2	AU-2 AU-2 (3) AU-2 (4)	<p>AU-2a. [Assignment: organization-defined list of auditable events] Parameter: [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes]</p> <p>AU-2d. [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited] Parameter: See additional requirements and guidance.</p> <p>AU-2d. [Assignment: organization-defined frequency of (or situation requiring) auditing for each identified event]. Parameter: [continually]</p> <p>AU-2 (3) [Assignment: organization-defined frequency] Parameter: [annually or whenever there is a change in the threat environment]</p>	<p>AU-2d. Requirement: The service provider defines the subset of auditable events from AU-2a to be audited. The events to be audited are approved and accepted by JAB.</p> <p>AU-2 (3) Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB.</p> <p>AU-2 Requirement: 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.</p>
AU-3	Content of Audit Records	AU-3	AU-3 AU-3 (1)	<p>AU-3 (1) [Assignment: organization-defined additional, more detailed information] Parameter: [session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]</p>	<p>AU-3 (1) Requirement: The service provider defines audit record types. The audit record types are approved and accepted by the JAB.</p> <p>Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.</p>
AU-4	Audit Storage Capacity	AU-4	AU-4	None.	None.
AU-5	Response to Audit Processing Failures	AU-5	AU-5	<p>AU-5b [Assignment: Organization-defined actions to be taken] Parameter: [low-impact: overwrite oldest audit records; moderate-impact: shut down]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AU-6	Audit Review, Analysis, and Reporting	AU-6	AU-6 AU-6 (1) AU-6 (3)	AU-6a. [Assignment: organization-defined frequency] Parameter: [at least weekly]	None.
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 AU-7 (1)	None.	None.
AU-8	Time Stamps	AU-8	AU-8 AU-8 (1)	AU-8 (1) [Assignment: organization-defined frequency] Parameter: [at least hourly] AU-8 (1) [Assignment: organization-defined authoritative time source] Parameter: [http://tf.nist.gov/tf-cgi/servers.cgi].	AU-8 (1) Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server. Guidance: Synchronization of system clocks improves the accuracy of log analysis.
AU-9	Protection of Audit Information	AU-9	AU-9 AU-9 (2)	AU-9 (2) [Assignment: organization-defined frequency] Parameter: [at least weekly]	None.
AU-10	Non-Repudiation	Not Selected	AU-10 AU-10 (5)	AU-10 (5) [Selection: FIPS-validated; NSA-approved] Parameter: See additional requirements and guidance.	AU-10 (5) Requirement: The service provider 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 email.
AU-11	Audit Record Retention	AU-11	AU-11	AU-11 [Assignment: organization-defined time period consistent with records retention policy] Parameter: [at least ninety days]	AU-11 Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AU-12	Audit Generation	AU-12	AU-12	AU-12a. [Assignment: organization-defined information system components] Parameter: [all information system components where audit capability is deployed]	None.
1.4. Assessment and Authorization (CA)					
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
CA-2	Security Assessments	CA-2 CA-2 (1)	CA-2 CA-2 (1)	CA-2b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
CA-3	Information System Connections	CA-3	CA-3	None.	None.
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5b. [Assignment: organization-defined frequency] Parameter: [at least quarterly]	None.
CA-6	Security Authorization	CA-6	CA-6	CA-6c. [Assignment: organization-defined frequency] Parameter: [at least every three years or when a significant change occurs]	CA-6c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a reauthorization of the information system. The types of changes are approved and accepted by the JAB.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CA-7	Continuous Monitoring	CA-7 CA-7 (2)	CA-7 CA-7 (2)	CA-7d. <i>[Assignment: organization-defined frequency]</i> Parameter: [monthly] CA-7 (2) <i>[Assignment: organization-defined frequency]</i> Parameter: [annually] <i>[Selection: announced; unannounced]</i> Parameter: [unannounced] <i>[Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises]</i> Parameter: [penetration testing] <i>[Assignment: organization-defined other forms of security assessment]</i> Parameter: [in-depth monitoring]	None.
1.5. Configuration Management (CM)					
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1 <i>[Assignment: organization-defined frequency]</i> Parameter: [at least annually]	None.
CM-2	Baseline Configuration	CM-2	CM-2 CM-2 (1) CM-2 (3) CM-2 (5)	CM-2 (1) (a) <i>[Assignment: organization-defined frequency]</i> Parameter: [annually] CM-2 (1) (b) <i>[Assignment: organization-defined circumstances]</i> Parameter: [a significant change] CM-2 (5) (a) <i>[Assignment: organization-defined list of software programs authorized to execute on the information system]</i> Parameter: See additional requirements and guidance.	CM-2 (1) (b) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a review and update of the baseline configuration. The types of changes are approved and accepted by the JAB. CM-2 (5) (a) Requirement: The service provider defines and maintains a list of software programs authorized to execute on the information system. The list of authorized programs is approved and accepted by the JAB.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CM-3	Configuration Change Control	CM-3	CM-3 CM-3 (2)	CM-3f. [Assignment: organization-defined configuration change control element] Parameter: See additional requirements and guidance. [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]] Parameter: See additional requirements and guidance.	CM-3f. Requirement: The service provider defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the JAB. Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB.
CM-4	Security Impact Analysis	CM-4	CM-4	None.	None.
CM-5	Access Restrictions for Change	Not Selected	CM-5 CM-5 (1) CM-5 (5)	CM-5 (5) (b) [Assignment: organization-defined frequency] Parameter: [at least quarterly]	None.
CM-6	Configuration Settings	CM-6	CM-6 CM-6 (1) CM-6 (3)	CM-6a. [Assignment: organization-defined security configuration checklists] Parameter: [United States Government Configuration Baseline (USGCB)]	CM-6a. Requirement: The service provider uses the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. Configuration settings are approved and accepted by the JAB. CM-6a Requirement: The service provider ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). CM-6a. Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc .

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CM-7	Least Functionality	CM-7	CM-7 CM-7 (1)	<p>CM-7 [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services] Parameter: [United States Government Configuration Baseline (USGCB)]</p> <p>CM-7 (1) [Assignment: organization-defined frequency] Parameter: [at least quarterly]</p>	<p>CM-7 Requirement: The service provider uses 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 is approved and accepted by the JAB.</p> <p>CM-7 Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc.</p>
CM-8	Information System Component Inventory	CM-8	CM-8 CM-8 (1) CM-8 (3) CM-8 (5)	<p>CM-8d. [Assignment: organization-defined information deemed necessary to achieve effective property accountability] Parameter: See additional requirements and guidance.</p> <p>CM-8 (3) (a) [Assignment: organization-defined frequency] Parameter: [Continuously, using automated mechanisms with a maximum five-minute delay in detection.]</p>	<p>CM-8d. Requirement: The service provider defines information deemed necessary to achieve effective property accountability. Property accountability information is approved and accepted by the JAB.</p> <p>Guidance: Information deemed necessary to achieve effective property accountability may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.</p>
CM-9	Configuration Management Plan		CM-9	None.	None.
1.6. Contingency Planning (CP)					
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	<p>CP-1 [Assignment: organization-defined frequency] Parameter: [at least annually]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CP-2	Contingency Plan	CP-2	CP-2 CP-2 (1) CP-2 (2)	<p>CP-2b. [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements] Parameter: See additional requirements and guidance.</p> <p>CP-2d. [Assignment: organization-defined frequency] Parameter: [at least annually]</p> <p>CP-2f. [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements] Parameter: See additional requirements and guidance.</p>	<p>CP-2b. Requirement: The service provider defines a list of key contingency personnel (identified by name and/or by role) and organizational elements. The contingency list includes designated FedRAMP personnel.</p> <p>CP-2f. Requirement: The service provider defines a list of key contingency personnel (identified by name and/or by role) and organizational elements. The contingency list includes designated FedRAMP personnel.</p>
CP-3	Contingency Training	CP-3	CP-3	<p>CP-3 [Assignment: organization-defined frequency] Parameter: [at least annually]</p>	None.
CP-4	Contingency Plan Testing and Exercises	CP-4	CP-4 CP-4 (1)	<p>CP-4a. [Assignment: organization-defined frequency] Parameter: [at least annually for moderate impact systems; at least every three years for low impact systems]</p> <p>[Assignment: organization-defined tests and/or exercises] Parameter: [functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems]</p>	<p>CP-4a. Requirement: 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.</p>
CP-6	Alternate Storage Site	Not Selected	CP-6 CP-6 (1) CP-6 (3)	None.	None.
CP-7	Alternate Processing Site	Not Selected	CP-7 CP-7 (1) CP-7 (2) CP-7 (3) CP-7 (5)	<p>CP-7a. [Assignment: organization-defined time period consistent with recovery time objectives] Parameter: See additional requirements and guidance.</p>	<p>CP-7a. Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the JAB.</p>

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CP-8	Telecommunications Services	Not Selected	CP-8 CP-8 (1) CP-8 (2)	CP-8 [Assignment: organization-defined time period] Parameter: See additional requirements and guidance.	CP-8 Requirement: The service provider defines a time period consistent with the business impact analysis. The time period is approved and accepted by the JAB.
CP-9	Information System Backup	CP-9	CP-9 CP-9 (1) CP-9 (3)	CP-9a. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [daily incremental; weekly full] CP-9b. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [daily incremental; weekly full] CP-9c. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [daily incremental; weekly full] CP-9 (1) [Assignment: organization-defined frequency] Parameter: [at least annually]	CP-9a. Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB. CP-9b. Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB. CP-9c. Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 CP-10 (2) CP-10 (3)	CP-10 (3) [Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state] Parameter: See additional requirements and guidance.	CP-10 (3) Requirement: 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.
1.7. Identification and Authentication (IA)					
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
IA-2	Identification and Authentication (Organizational Users)	IA-2 IA-2 (1)	IA-2 IA-2 (1) IA-2 (2) IA-2 (3) IA-2 (8)	IA-2 (8) [Assignment: organization-defined replay-resistant authentication mechanisms] Parameter: See additional requirements and guidance.	IA-2 (8) Requirement: The service provider defines replay-resistant authentication mechanisms. The mechanisms are approved and accepted by the JAB.
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3 [Assignment: organization-defined list of specific and/or types of devices] Parameter: See additional requirements and guidance.	IA-3 Requirement: The service provider defines a list a specific devices and/or types of devices. The list of devices and/or device types is approved and accepted by the JAB.
IA-4	Identifier Management	IA-4	IA-4 IA-4 (4)	IA-4d. [Assignment: organization-defined time period] Parameter: [at least two years] IA-4e. [Assignment: organization-defined time period of inactivity] Parameter: [ninety days for user identifiers] Parameter: See additional requirements and guidance. IA-4 (4) [Assignment: organization-defined characteristic identifying user status] Parameter: [contractors; foreign nationals]	IA-4e. Requirement: The service provider defines time period of inactivity for device identifiers. The time period is approved and accepted by JAB.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
IA-5	Authenticator Management	IA-5 IA-5 (1)	IA-5 IA-5 (1) IA-5 (2) IA-5 (3) IA-5 (6) IA-5 (7)	<p>IA-5g. [Assignment: organization-defined time period by authenticator type] Parameter: [sixty days]</p> <p>IA-5 (1) (a) [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type] Parameter: [case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters]</p> <p>IA-5 (1) (b) [Assignment: organization-defined number of changed characters] Parameter: [at least one or as determined by the information system (where possible)]</p> <p>IA-5 (1) (d) [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum] Parameter: [one day minimum, sixty day maximum]</p> <p>IA-5 (1) (e) [Assignment: organization-defined number] Parameter: [twenty four]</p> <p>IA-5 (3) [Assignment: organization-defined types of and/or specific authenticators] Parameter: [HSPD12 smart cards]</p>	IA-5 (1) (a) Guidance: Mobile devices are excluded from the password complexity requirement.
IA-6	Authenticator Feedback	IA-6	IA-6	None.	None.
IA-7	Cryptographic Module Authentication	IA-7	IA-7	None.	None.
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8	IA-8	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
1.8. Incident Response (IR)					
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
IR-2	Incident Response Training	IR-2	IR-2	IR-2b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 [Assignment: organization-defined frequency] Parameter: [annually] [Assignment: organization-defined tests and/or exercises] Parameter: See additional requirements and guidance.	IR-3 Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). IR-3 Requirement: The service provider provides test plans to FedRAMP annually. Test plans are approved and accepted by the JAB prior to test commencing.
IR-4	Incident Handling	IR-4	IR-4 IR-4 (1)	None.	IR-4 Requirement: 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	IR-5	IR-5	None.	None.
IR-6	Incident Reporting	IR-6	IR-6 IR-6 (1)	IR-6a. [Assignment: organization-defined time period] Parameter: [US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
IR-7	Incident Response Assistance	IR-7	IR-7 IR-7 (1) IR-7 (2)	None.	None.
IR-8	Incident Response Plan	IR-8	IR-8	<p>IR-8b. [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements] Parameter: See additional requirements and guidance.</p> <p>IR-8c. [Assignment: organization-defined frequency] Parameter: [at least annually]</p> <p>IR-8e. [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements] Parameter: See additional requirements and guidance.</p>	<p>IR-8b. Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.</p> <p>IR-8e. Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.</p>
1.9. Maintenance (MA)					
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
MA-2	Controlled Maintenance	MA-2	MA-2 MA-2 (1)	None.	None.
MA-3	Maintenance Tools	Not Selected	MA-3 MA-3 (1) MA-3 (2) MA-3 (3)	None.	None.
MA-4	Non-Local Maintenance	MA-4	MA-4 MA-4 (1) MA-4 (2)	None.	None.
MA-5	Maintenance Personnel	MA-5	MA-5	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
MA-6	Timely Maintenance	Not Selected	MA-6	<p>MA-6 [Assignment: organization-defined list of security-critical information system components and/or key information technology components] Parameter: See additional requirements and guidance.</p> <p>[Assignment: organization-defined time period] Parameter: See additional requirements and guidance.</p>	<p>MA-6 Requirement: The service provider defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the JAB.</p> <p>Requirement: The service provider defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the JAB.</p>
1.10. Media Protection (MP)					
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	<p>MP-1 [Assignment: organization-defined frequency] Parameter: [at least annually]</p>	None.
MP-2	Media Access	MP-2	MP-2 MP-2 (1)	<p>MP-2 [Assignment: organization-defined types of digital and non-digital media] Parameter: See additional requirements and guidance.</p> <p>[Assignment: organization-defined list of authorized individuals] Parameter: See additional requirements and guidance.</p> <p>[Assignment: organization-defined security measures] Parameter: See additional requirements and guidance.</p>	<p>MP-2 Requirement: The service provider defines types of digital and non-digital media. The media types are approved and accepted by the JAB.</p> <p>Requirement: The service provider defines a list of individuals with authorized access to defined media types. The list of authorized individuals is approved and accepted by the JAB.</p> <p>Requirement: The service provider defines the types of security measures to be used in protecting defined media types. The security measures are approved and accepted by the JAB.</p>
MP-3	Media Marking	Not Selected	MP-3	<p>MP-3b. [Assignment: organization-defined list of removable media types] Parameter: [no removable media types]</p> <p>[Assignment: organization-defined controlled areas] Parameter: [not applicable]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
MP-4	Media Storage	Not Selected	MP-4 MP-4 (1)	MP-4a. <i>[Assignment: organization-defined types of digital and non-digital media]</i> Parameter: [magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks] <i>[Assignment: organization-defined controlled areas]</i> Parameter: See additional requirements and guidance. <i>[Assignment: organization-defined security measures]</i> Parameter: [for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secure storage in locked cabinets or safes]	MP-4a. Requirement: The service provider defines controlled areas within facilities where the information and information system reside.
MP-5	Media Transport	Not Selected	MP-5 MP-5 (2) MP-5 (4)	MP-5a. <i>[Assignment: organization-defined types of digital and non-digital media]</i> Parameter: [magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks] <i>[Assignment: organization-defined security measures]</i> Parameter: [for digital media, encryption using a FIPS 140-2 validated encryption module]	MP-5a. Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB.
MP-6	Media Sanitization	MP-6	MP-6 MP-6 (4)	None.	None.
1.11. Physical and Environmental Protection (PE)					
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1 <i>[Assignment: organization-defined frequency]</i> Parameter: [at least annually]	None.
PE-2	Physical Access Authorizations	PE-2	PE-2 PE-2 (1)	PE-2c. <i>[Assignment: organization-defined frequency]</i> Parameter: [at least annually]	PE-2 (1) Requirement: The service provider provides physical access to the facility where information systems reside based on position, role, and need-to-know.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PE-3	Physical Access Control	PE-3	PE-3	PE-3f. [Assignment: organization-defined frequency] Parameter: [at least annually] PE-3g. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PE-4	Access Control for Transmission Medium	Not Selected	PE-4	None.	None.
PE-5	Access Control for Output Devices	Not Selected	PE-5	None.	None.
PE-6	Monitoring Physical Access	PE-6	PE-6 PE-6 (1)	PE-6b. [Assignment: organization-defined frequency] Parameter: [at least semi-annually]	None.
PE-7	Visitor Control	PE-7	PE-7 PE-7 (1)	None.	None.
PE-8	Access Records	PE-8	PE-8	PE-8b. [Assignment: organization-defined frequency] Parameter: [at least monthly]	None.
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	None.	None.
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10b. [Assignment: organization-defined location by information system or system component] Parameter: See additional requirements and guidance.	PE-10b. Requirement: The service provider defines emergency shutoff switch locations. The locations are approved and accepted by the JAB.
PE-11	Emergency Power	Not Selected	PE-11 PE-11 (1)	None.	None.
PE-12	Emergency Lighting	PE-12	PE-12	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PE-13	Fire Protection	PE-13	PE-13 PE-13 (1) PE-13 (2) PE-13 (3)	None.	None.
PE-14	Temperature and Humidity Controls	PE-14	PE-14 PE-14 (1)	PE-14a. [Assignment: organization-defined acceptable levels] Parameter: [consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled <i>Thermal Guidelines for Data Processing Environments</i>] PE-14b. [Assignment: organization-defined frequency] Parameter: [continuously]	PE-14a. Requirements: The service provider measures temperature at server inlets and humidity levels by dew point.
PE-15	Water Damage Protection	PE-15	PE-15	None.	None.
PE-16	Delivery and Removal	PE-16	PE-16	PE-16 [Assignment: organization-defined types of information system components] Parameter: [all information system components]	None.
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17a. [Assignment: organization-defined management, operational, and technical information system security controls] Parameter: See additional requirements and guidance.	PE-17a. Requirement: The service provider defines management, operational, and technical information system security controls for alternate work sites. The security controls are approved and accepted by the JAB.
PE-18	Location of Information System Components	Not Selected	PE-18	None.	None.
1.12. Planning (PL)					
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PL-2	System Security Plan	PL-2	PL-2 PL-2 (2)	PL-2b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PL-4	Rules of Behavior	PL-4	PL-4	None.	None.
PL-5	Privacy Impact Assessment	PL-5	PL-5	None.	None.
PL-6	Security-Related Activity Planning	PL-6	PL-6	None.	None.
1.13. Personnel Security (PS)					
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PS-2	Position Categorization	PS-2	PS-2	PS-2c. [Assignment: organization-defined frequency] Parameter: [at least every three years]	None.
PS-3	Personnel Screening	PS-3	PS-3	PS-3b. [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening] Parameter: [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]	None.
PS-4	Personnel Termination	PS-4	PS-4	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PS-5	Personnel Transfer	PS-5	PS-5	PS-5 [Assignment: organization-defined transfer or reassignment actions] Parameter: See additional requirements and guidance. [Assignment: organization-defined time period following the formal transfer action] Parameter: [within five days]	PS-5 Requirement: The service provider defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the JAB.
PS-6	Access Agreements	PS-6	PS-6	PS-6b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PS-7	Third-Party Personnel Security	PS-7	PS-7	None.	None.
PS-8	Personnel Sanctions	PS-8	PS-8	None.	None.
1.14. Risk Assessment (RA)					
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
RA-2	Security Categorization	RA-2	RA-2	None.	None.
RA-3	Risk Assessment	RA-3	RA-3	RA-3b. [Selection: security plan; risk assessment report; [Assignment: organization-defined document]] Parameter: [security assessment report] RA-3c. [Assignment: organization-defined frequency] Parameter: [at least every three years or when a significant change occurs] RA-3d. [Assignment: organization-defined frequency] Parameter: [at least every three years or when a significant change occurs]	RA-3c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. RA-3d. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
RA-5	Vulnerability Scanning	RA-5 RA-5 (1) RA-5 (2) RA-5 (3) RA-5 (9)	RA-5 RA-5 (1) RA-5 (2) RA-5 (3) RA-5 (9) RA-5 (6)	RA-5a. [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] Parameter: [quarterly operating system, web application, and database scans (as applicable)] RA-5d. Assignment: organization-defined response times Parameter: [high-risk vulnerabilities mitigated within thirty days; moderate risk vulnerabilities mitigated within ninety days] RA-5 (2) [Assignment: organization-defined frequency] Parameter: [continuously, before each scan]	None.
1.15. System and Services Acquisition (SA)					
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
SA-2	Allocation of Resources	SA-2	SA-2	None.	None.
SA-3	Life Cycle Support	SA-3	SA-3	None.	None.
SA-4	Acquisitions	SA-4	SA-4 SA-4 (1) SA-4 (4) SA-4 (7)	None.	SA-4 Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See http://www.niap-ccevs.org/vpl or http://www.commoncriteriaportal.org/products.html .
SA-5	Information System Documentation	SA-5	SA-5 SA-5 (1) SA-5 (3)	None.	None.
SA-6	Software Usage Restrictions	SA-6	SA-6	None.	None.
SA-7	User-Installed Software	SA-7	SA-7	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SA-8	Security Engineering Principles	Not Selected	SA-8	None.	None.
SA-9	External Information System Services	SA-9	SA-9 SA-9 (1)	SA-9 (1) (b) [Assignment: organization-defined senior organizational official]. Parameter: [Joint Authorization Board (JAB)]	SA-9 (1) Requirement: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. Future, planned outsourced services are approved and accepted by the JAB.
SA-10	Developer Configuration Management	Not Selected	SA-10	None.	None.
SA-11	Developer Security Testing	SA-11 SA-11 (1)	SA-11 SA-11 (1)	None.	SA-11 (1) Requirement: The service provider submits a code analysis report as part of the authorization package and updates the report in any reauthorization actions. SA-11 (1) Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.
SA-12	Supply Chain Protection	Not Selected	SA-12	SA-12 [Assignment: organization-defined list of measures to protect against supply chain threats] Parameter: See additional requirements and guidance.	SA-12 Requirement: The service provider defines a list of measures to protect against supply chain threats. The list of protective measures is approved and accepted by JAB.
1.16. System and Communications Protection (SC)					
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-2	Application Partitioning	Not Selected	SC-2	None.	None.
SC-4	Information in Shared Resources	Not Selected	SC-4	None.	None.
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5 [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list] Parameter: See additional requirements and guidance.	SC-5 Requirement: The service provider defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by JAB.
SC-6	Resource Priority	Not Selected	SC-6	None	None.
SC-7	Boundary Protection	SC-7	SC-7 SC-7 (1) SC-7 (2) SC-7 (3) SC-7 (4) SC-7 (5) SC-7 (7) SC-7 (8) SC-7 (12) SC-7 (13) SC-7 (18)	SC-7 (4) (e) [Assignment: organization-defined frequency] Parameter: [at least annually] SC-7 (8) [Assignment: organization-defined internal communications traffic] Parameter: See additional requirements and guidance. [Assignment: organization-defined external networks] Parameter: See additional requirements and guidance. SC-7 (13) [Assignment: organization-defined key information security tools, mechanisms, and support components] Parameter: See additional requirements and guidance.	SC-7 (1) Requirement: 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 (8) Requirements: The service provider defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by JAB. SC-7 (13) Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-8	Transmission Integrity	Not Selected	SC-8 SC-8 (1)	None.	None.
SC-9	Transmission Confidentiality	Not Selected	SC-9 SC-9 (1)	SC-9 (1) [Assignment: <i>organization-defined alternative physical measures</i>] Parameter: See additional requirements and guidance	SC-9(1) Requirement: 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	Not Selected	SC-10	SC-10 [Assignment: <i>organization-defined time period</i>] Parameter: [thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users]	SC-10 Guidance: Long running batch jobs and other operations are not subject to this time limit.
SC-11	Trusted Path	Not Selected	SC-11	SC-11 [Assignment: <i>organization-defined security functions to include at a minimum, information system authentication and re-authentication</i>] Parameter: See additional requirements and guidance	SC-11 Requirement: The service provider defines the security functions that require a trusted path, including but not limited to system authentication, re-authentication, and provisioning or de-provisioning of services (i.e. allocating additional bandwidth to a cloud user). The list of security functions requiring a trusted path is approved and accepted by JAB.
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12 SC-12 (2) SC-12 (5)	SC-12 (2) [Selection: <i>NIST-approved, NSA-approved</i>] Parameter: [NIST-approved]	None.
SC-13	Use of Cryptography	SC-13	SC-13 SC-13 (1)	None.	None.
SC-14	Public Access Protections	SC-14	SC-14	None.	None.
SC-15	Collaborative Computing Devices	SC-15	SC-15	SC-15a. [Assignment: <i>organization-defined exceptions where remote activation is to be allowed</i>] Parameter: [no exceptions]	SC-15 Requirement: The information system provides <i>disablement</i> (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-16	Transmission of Security Attributes	Not Selected	SC-16	None.	None.
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17 [Assignment: <i>organization-defined certificate policy</i>] Parameter: See additional requirements and guidance.	SC-17 Requirement: The service provider defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the JAB.
SC-18	Mobile Code	SC-18	SC-18 SC-18 (4)	SC-18 (4) [Assignment: <i>organization-defined software applications</i>] Parameter: See additional requirements and guidance. [Assignment: <i>organization-defined actions</i>] Parameter: See additional requirements and guidance.	SC-18 (4) Requirement: The service provider defines the software applications where the automatic execution of mobile code is prevented by the information system providing cloud services. Requirement: The service provider defines the actions to be taken prior to the information system executing mobile code in the software applications identified. Software applications and actions taken by the service provider are approved by JAB.
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	None.	None.
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20 SC-20 (1)	SC-20 SC-20 (1)	None.	None.
SC-21	Secure Name/ Address Resolution Service (Recursive or Caching Resolver)	Not Selected	SC-21	None.	None.
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	None.	None.
SC-23	Session Authenticity	Not Selected	SC-23	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-25	Thin Nodes	Not Selected	SC-25	None	None.
SC-27	Operating System-Independent Applications	Not Selected	SC-27	SC-27 [Assignment: organization-defined operating system independent applications]. Parameter: See additional requirements and guidance	SC-27 Requirement: The service provider and service consumer define which applications must run independent of operating system. The OS Independent applications list is approved and accepted by JAB.
SC-28	Protection of Information at Rest	Not Selected	SC-28 SC-28 (1)	None.	None.
SC-30	Virtualization Techniques	Not Selected	SC-30	None	None.
SC-32	Information System Partitioning	Not Selected	SC-32	None.	None.
SC-33	Transmission Preparation Integrity	Not Selected	SC-33	None.	None.
1.17. System and Information Integrity (SI)					
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
SI-2	Flaw Remediation	SI-2	SI-2 SI-2 (2)	SI-2 (2) [Assignment: organization-defined frequency] Parameter: [at least monthly]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SI-3	Malicious Code Protection	SI-3	SI-3 SI-3 (1) SI-3 (2) SI-3 (3)	SI-3c. [Assignment: organization-defined frequency] Parameter: [at least weekly] [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] Parameter: [block or quarantine malicious code, send alert to administrator, send alert to FedRAMP]	None.
SI-4	Information System Monitoring	SI-4	SI-4 SI-4 (2) SI-4 (4) SI-4 (5) SI-4 (6)	SI-4a. [Assignment: organization-defined monitoring objectives] Parameter: [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] SI-4 (5) [Assignment: organization-defined list of compromise indicators] Parameter: [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]	SI-4(5) Requirement: The service provider defines additional compromise indicators as needed. Guidance: Alerts may be generated from a variety of sources including but not limited to malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5	SI-5c. [Assignment: organization-defined list of personnel (identified by name and/or by role)] Parameter: [All staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP]	SI-5c. Requirement: The service provider defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated FedRAMP personnel.
SI-6	Security functionality verification	Not Selected	SI-6	SI-6 [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] Parameter: [upon system startup and/or restart and periodically every ninety days] [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] Parameter: [notifies system administrator]	None.
SI-7	Software and Information Integrity	Not Selected	SI-7 SI-7 (1)	SI-7 (1) [Assignment: organization-defined frequency] Parameter: [at least monthly]	None.
SI-8	Spam Protection	Not Selected	SI-8	None.	None.
SI-9	Information Input Restrictions	Not Selected	SI-9	None.	None.
SI-10	Information Input Validation	SI-10	SI-10	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SI-11	Error Handling	Not Selected	SI-11	SI-11b. [Assignment: organization-defined sensitive or potentially harmful information] Parameter: [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)].	None.
SI-12	Information Output Handling and Retention	SI-12	SI-12	None.	None.

Table 1: FedRAMP Security Controls & Enhancements.