|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | A blue and white logo  Description automatically generated with medium confidence | |  | |
|  |  | | |  |
|  | FedRAMP® System Security Plan (SSP) Appendix A: LI-SaaS FedRAMP Security Controls  for <Insert CSP Name>  <Insert CSO Name>  <Insert Version X.X>  <Insert MM/DD/YYYY> | | |  |
|
|  |  | | |  |
|  | A picture containing screenshot, font, graphics, logo  Description automatically generated | info@fedramp.gov  fedramp.gov | |  |

TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 06/30/2023 | 1.0 | All | Initial publication. SSP security control sections are now provided as separate templates. | FedRAMP PMO |
| 8/30/2023 | 1.1 | All | Updated template to resolve formatting issues, updated checkbox style and replaced reference to Test Case Workbook to Penetration Test Report. | FedRAMP PMO |

**How to contact us**

For questions about FedRAMP, or for questions about this document including how to use it, contact [info@FedRAMP.gov.](mailto:info@FedRAMP.gov)

For more information about FedRAMP, see [www.FedRAMP.gov](http://www.fedramp.gov).

Delete this Template Revision History page and all other instructional text from your final version of this document.

Appendix A LI-SaaS: <CSO Name> FedRAMP Security Controls

Security controls must meet minimum security control baseline requirements. The following table contains the FedRAMP *Tailored* LI-SaaS Security Controls Baseline (by family).

There are six (6) categories of FedRAMP *Tailored* LI-SaaS controls: FED, NSO, Required, Conditional, Inherited, and Attestation. Table A-1, Control Tailoring Criteria, provides definitions of the tailoring criteria utilized for the determination of the FedRAMP *Tailored* LI-SaaS baseline.

Table A-1. Control Tailoring Criteria

| **Tailoring Symbol** | **Tailoring Criteria** | **CSP Response Requirements** |
| --- | --- | --- |
| **FED** | The control is typically the responsibility of the Federal Government, not the CSP. | No CSP response is required. |
| **NSO** | FedRAMP has determined the control does not impact the security of a SaaS cloud offering. | No CSP response is required. |
| **Document and Assess** | The control must be documented in Appendix B, and independently assessed.  This does not mean that a vendor will necessarily have each control fully implemented or implemented as stated. A vendor must address how they meet (or don't meet) the intent of the control so that it can be independently assessed and detail any risks associated with the implementation. | A CSP must provide documentation for the control below. |
| **Document and Assess (D&A) Conditional** | If the condition exists, the control must be documented in Appendix B and independently assessed as above. If the condition does not exist, a CSP must attest to this in Appendix E. | A CSP must provide documentation for the control below. |
| **Inherited** | The control is inherited from the underlying infrastructure provider (i.e., FedRAMP Authorized IaaS/PaaS). | A CSP attestation response is required. |
| **Attest** | A CSP may attest to the existence of the control in Appendix E. No documentation, nor independent assessment is required. | A CSP attestation response is required. |

A CSP response, for all controls requiring an attestation of the status and implementation of the security requirements, is defined in the FedRAMP *Tailored* LI-SaaS CSP Self-Attestation table. (See Section 3, FedRAMP *Tailored* Low Impact Software as a Service [LI-SaaS] Self-Attestation Requirements).

Table A-2, Summary of FedRAMP *Tailored* LI-SaaS Security Controls, lists all the controls required for the FedRAMP Low Impact Baseline and the associated tailoring criteria for each control.

Table A-2. Summary of FedRAMP Tailored LI-SaaS Security Controls

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Control Description | FedRAMP *Tailored* LI-SaaS Controls | | | | | | |
| **FED** | **NSO** | **Document and Assess** | **D&A Conditional** | | **Inherited** | **Attest** |
| **AC – Access Control** | | | | | | | | |
| **AC-1** | Policy and Procedures |  |  |  |  | |  | x |
| **AC-2** | Account Management |  |  | x |  | |  |  |
| **AC-3** | Access Enforcement |  |  | x |  | |  |  |
| **AC-7** | Unsuccessful Logon Attempts |  | x | x |  | |  |  |
| **AC-8** | System Use Notification | x |  |  |  | |  |  |
| **AC-14** | Permitted Actions Without Identification or Authentication | x |  |  |  | |  |  |
| **AC-17** | Remote Access |  |  | x |  | |  |  |
| **AC-18** | Wireless Access |  | x |  |  | |  |  |
| **AC-19** | Access Control for Mobile Devices |  | x |  |  | |  |  |
| **AC-20** | Use of External Systems |  |  |  |  | |  | x |
| **AC-22** | Publicly Accessible Content |  |  | x |  | |  |  |
| **AT – Awareness and Training** | | | | | | | | |
| **AT-1** | Policy and Procedures |  |  |  | |  |  | x |
| **AT-2** | Literacy Training and Awareness |  |  |  | |  |  | x |
| **AT-2(2)** | Insider Threat |  |  |  | |  |  | x |
| **AT-3** | Role-based Training |  |  |  | |  |  | x |
| **AT-4** | Training Records |  |  |  | |  |  | x |
| **AU – Audit and Accountability** | | | | | | | | |
| **AU-1** | Policy and Procedures |  |  |  | |  |  | x |
| **AU-2** | Event Logging |  |  |  | |  |  | x |
| **AU-3** | Content of Audit Records |  |  | x | |  |  |  |
| **AU-4** | Audit Log Storage Capacity |  | x |  | |  |  |  |
| **AU-5** | Response to Audit Logging Process Failures |  |  | x | |  |  |  |
| **AU-6** | Audit Record Review, Analysis, and Reporting |  |  | x | |  |  |  |
| **AU-8** | Time Stamps |  |  |  | |  |  | x |
| **AU-9** | Protection of Audit Information |  |  |  | |  |  | x |
| **AU-11** | Audit Record Retention |  | x |  | |  |  |  |
| **AU-12** | Audit Record Generation |  |  |  | |  |  | x |
| **CA – Security Assessment, Authorization, and Monitoring** | | | | | | | | |
| **CA-1** | Policy and Procedures |  |  |  | |  |  | x |
| **CA-2** | Control Assessments |  |  | x | |  |  |  |
| **CA-2(1)** | Independent Assessors |  |  |  | |  |  | x |
| **CA-3** | Information Exchange |  |  |  | | x |  |  |
| **CA-5** | Plan of Action and Milestones |  |  |  | |  |  | x |
| **CA-6** | Authorization |  |  | x | |  |  |  |
| **CA-7** | Continuous Monitoring |  |  | x | |  |  |  |
| **CA-7(4)** | Risk Monitoring |  |  | x | |  |  |  |
| **CA-8** | Penetration Testing |  |  | x | |  |  |  |
| **CA-9** | Internal System Connections |  |  |  | | x |  |  |
| **CM – Configuration Management** | | | | | | | | |
| **CM-1** | Policy and Procedures |  |  |  | |  |  | x |
| **CM-2** | Baseline Configuration |  |  |  | |  |  | x |
| **CM-4** | Impact Analyses |  |  | x | |  |  |  |
| **CM-5** | Access Restrictions for Change |  |  | x | |  |  |  |
| **CM-6** | Configuration Settings |  |  | x | |  |  |  |
| **CM-7** | Least Functionality |  |  |  | |  |  | x |
| **CM-8** | System Component Inventory |  |  | x | |  |  |  |
| **CM-10** | Software Usage Restrictions |  | x |  | |  |  |  |
| **CM-11** | User-installed Software |  | x |  | |  |  |  |
| **CP – Contingency Planning** | | | | | | | | |
| **CP-1** | Policy and Procedures |  |  |  | |  |  | x |
| **CP-2** | Contingency Plan |  | x |  | |  |  |  |
| **CP-3** | Contingency Training |  | x |  | |  |  |  |
| **CP-4** | Contingency Plan Testing |  | x |  | |  |  |  |
| **CP-9** | System Backup |  |  | x | |  |  |  |
| **CP-10** | System Recovery and Reconstitution |  | x |  | |  |  |  |
| **IA – Identification and Authentication** | | | | | | | | |
| **IA-1** | Policy and Procedures |  |  |  | |  |  | x |
| **IA-2** | Identification and Authentication (Organizational Users) |  | x |  | |  |  | x |
| **IA-2(1)** | Multi-factor Authentication to Privileged Accounts |  |  | x | |  |  |  |
| **IA-2(2)** | Multi-factor Authentication to Non-privileged Accounts |  |  | x | |  |  |  |
| **IA-2(8)** | Access to Accounts — Replay Resistant |  |  | x | |  |  |  |
| **IA-2(12)** | Acceptance of PIV Credentials |  |  | x | |  |  |  |
| **IA-4** | Identifier Management |  |  |  | |  |  | x |
| **IA-5** | Authenticator Management |  |  |  | |  |  | x |
| **IA-5(1)** | Password-based Authentication |  |  |  | |  |  | x |
| **IA-6** | Authentication Feedback |  |  | x | |  |  |  |
| **IA-7** | Cryptographic Module Authentication |  |  | x | |  |  |  |
| **IA-8** | Identification and Authentication (Non-organizational Users) |  |  |  | |  |  | x |
| **IA-8(1)** | Acceptance of PIV Credentials from Other Agencies |  |  |  | | x |  |  |
| **IA-8(2)** | Acceptance of External Authenticators |  |  |  | | x |  |  |
| **IA-8(4)** | Use of Defined Profiles |  |  |  | |  |  | x |
| **IA-11** | Re-authentication |  |  |  | |  |  | x |
| **IR – Incident Response** | | | | | | | | |
| **IR-1** | Policy and Procedures |  |  |  | |  |  | x |
| **IR-2** | Incident Response Training |  |  |  | |  |  | x |
| **IR-4** | Incident Handling |  |  | x | |  |  |  |
| **IR-5** | Incident Monitoring |  |  |  | |  |  | x |
| **IR-6** | Incident Reporting |  |  | x | |  |  |  |
| **IR-7** | Incident Response Assistance |  |  |  | |  |  | x |
| **IR-8** | Incident Response Plan |  |  |  | |  |  | x |
| **MA – Maintenance** | | | | | | | | |
| **MA-1** | Policy and Procedures |  |  |  | |  |  | x |
| **MA-2** | Controlled Maintenance |  |  |  | | x | x |  |
| **MA-4** | Nonlocal Maintenance |  |  |  | |  |  | x |
| **MA-5** | Maintenance Personnel |  |  |  | | x | x |  |
| **MP – Media Protection** | | | | | | | | |
| **MP-1** | Policy and Procedures |  |  |  | |  |  | x |
| **MP-2** | Media Access |  |  |  | | x | x |  |
| **MP-6** | Media Sanitization |  |  |  | | x | x |  |
| **MP-7** | Media Use |  |  |  | | x | x |  |
| **PE – Physical and Environmental Protection** | | | | | | | | |
| **PE-1** | Policy and Procedures |  |  |  | |  |  | x |
| **PE-2** | Physical Access Authorizations |  |  |  | | x | x |  |
| **PE-3** | Physical Access Control |  |  |  | | x | x |  |
| **PE-6** | Monitoring Physical Access |  |  |  | | x | x |  |
| **PE-8** | Visitor Access Records |  |  |  | | x | x |  |
| **PE-12** | Emergency Lighting |  |  |  | | x | x |  |
| **PE-13** | Fire Protection |  |  |  | | x | x |  |
| **PE-14** | Environmental Controls |  |  |  | | x | x |  |
| **PE-15** | Water Damage Protection |  |  |  | | x | x |  |
| **PE-16** | Delivery and Removal |  |  |  | | x | x |  |
| **PL – Planning** | | | | | | | | |
| **PL-1** | Policy and Procedures |  |  |  | |  |  | x |
| **PL-2** | System Security and Privacy Plans |  |  | x | |  |  |  |
| **PL-4** | Rules of Behavior |  |  |  | |  |  | x |
| **PL-4(1)** | Social Media and External Site/Application Usage Restrictions |  |  |  | |  |  | x |
| **PL-8** | Security and Privacy Architectures |  |  | x | |  |  |  |
| **PL-10** | Baseline Selection |  |  |  | |  |  | x |
| **PL-11** | Baseline Tailoring |  |  |  | |  |  | x |
| **PS – Personnel Security** | | | | | | | | |
| **PS-1** | Policy and Procedures |  |  |  | |  |  | x |
| **PS-2** | Position Risk Designation | x |  |  | |  |  |  |
| **PS-3** | Personnel Screening |  |  | x | |  |  |  |
| **PS-4** | Personnel Termination |  |  |  | |  |  | x |
| **PS-5** | Personnel Transfer |  |  |  | |  |  | x |
| **PS-6** | Access Agreements |  |  |  | |  |  | x |
| **PS-7** | External Personnel Security |  |  |  | |  |  | x |
| **PS-8** | Personnel Sanctions |  |  |  | |  |  | x |
| **PS-9** | Position Descriptions |  |  |  | |  |  | x |
| **RA – Risk Assessment** | | | | | | | | |
| **RA-1** | Policy and Procedures |  |  |  | |  |  | x |
| **RA-2** | Security Categorization |  |  | x | |  |  |  |
| **RA-3** | Risk Assessment |  |  | x | |  |  |  |
| **RA-3(1)** | Supply Chain Risk Assessment |  |  |  | |  |  | x |
| **RA-5** | Vulnerability Monitoring and Scanning |  |  | x | |  |  |  |
| **RA-5(2)** | Update Vulnerabilities to Be Scanned |  |  | x | |  |  |  |
| **RA-5(11)** | Public Disclosure Program |  |  | x | |  |  |  |
| **RA-7** | Risk Response |  |  | x | |  |  |  |
| **SA – System and Services Acquisition** | | | | | | | | |
| **SA-1** | Policy and Procedures |  |  |  | |  |  | x |
| **SA-2** | Allocation of Resources |  |  |  | |  |  | x |
| **SA-3** | System Development Life Cycle |  |  |  | |  |  | x |
| **SA-4** | Acquisition Process |  |  |  | |  |  | x |
| **SA-4(10)** | Use of Approved PIV Products |  |  |  | |  |  | x |
| **SA-5** | System Documentation |  |  |  | |  |  | x |
| **SA-8** | Security and Privacy Engineering Principles |  |  |  | |  |  | x |
| **SA-9** | External System Services |  |  | x | |  |  |  |
| **SA-22** | Unsupported System Components |  |  | x | |  |  |  |
| **SC – System and Communications Protection** | | | | | | | | |
| **SC-1** | Policy and Procedures |  |  |  | |  |  | x |
| **SC-5** | Denial-of-service Protection |  |  |  | | x |  |  |
| **SC-7** | Boundary Protection |  |  | x | |  |  |  |
| **SC-8** | Transmission Confidentiality and Integrity |  |  | x | |  |  |  |
| **SC-8(1)** | Cryptographic Protection |  |  | x | |  |  |  |
| **SC-12** | Cryptographic Key Establishment and Management |  |  | x | |  |  |  |
| **SC-13** | Cryptographic Protection |  |  |  | | x |  |  |
| **SC-15** | Collaborative Computing Devices and Applications |  | x |  | |  |  |  |
| **SC-20** | Secure Name/Address Resolution Service (Authoritative Source) |  |  |  | |  |  | x |
| **SC-21** | Secure Name/Address Resolution Service (Recursive or Caching Resolver) |  |  |  | |  |  | x |
| **SC-22** | Architecture and Provisioning for Name/Address Resolution Service |  |  |  | |  |  | x |
| **SC-28** | Protection of Information at Rest |  |  | x | |  |  |  |
| **SC-28(1)** | Cryptographic Protection |  |  | x | |  |  |  |
| **SC-39** | Process Isolation |  |  |  | |  |  | x |
| **SI – System and Information Integrity** | | | | | | | | |
| **SI-1** | Policy and Procedures |  |  |  | |  |  | x |
| **SI-2** | Flaw Remediation |  |  | x | |  |  |  |
| **SI-3** | Malicious Code Protection |  |  | x | |  |  |  |
| **SI-4** | System Monitoring |  |  | x | |  |  |  |
| **SI-5** | Security Alerts, Advisories, and Directives |  |  |  | |  |  | x |
| **SI-12** | Information Management and Retention |  |  |  | |  |  | x |
| **SR - Supply Chain Risk Management** | | | | | | | | |
| **SR-1** | Policy and Procedures |  |  |  | |  |  | x |
| **SR-2** | Supply Chain Risk Management Plan |  |  |  | |  |  | x |
| **SR-2(1)** | Establish SCRM Team |  |  |  | |  |  | x |
| **SR-3** | Supply Chain Controls and Processes |  |  |  | |  |  | x |
| **SR-5** | Acquisition Strategies, Tools, and Methods |  |  |  | |  |  | x |
| **SR-8** | Notification Agreements |  |  |  | |  |  | x |
| **SR-10** | Inspection of Systems or Components |  |  |  | |  |  | x |
| **SR-11** | Component Authenticity |  |  |  | |  |  | x |
| **SR-11(1)** | Anti-counterfeit Training |  |  |  | |  |  | x |
| **SR-11(2)** | Configuration Control for Component Service and Repair |  |  |  | |  |  | x |
| **SR-12** | Component Disposal |  |  |  | |  |  | x |

TABLE OF CONTENTS

[1.0 Documented and Assessed Controls 23](#_Toc144300871)

[Access Control (AC) 27](#_Toc144300872)

[AC-2 Account Management 27](#_Toc144300873)

[AC-3 Access Enforcement 31](#_Toc144300874)

[AC-7 Unsuccessful Logon Attempts 32](#_Toc144300875)

[AC-17 Remote Access 35](#_Toc144300876)

[AC-22 Publicly Accessible Content 37](#_Toc144300877)

[Audit and Accountability (AU) 39](#_Toc144300878)

[AU-3 Content of Audit Records 39](#_Toc144300879)

[AU-5 Response to Audit Logging Process Failures 42](#_Toc144300880)

[AU-6 Audit Record Review, Analysis, and Reporting 44](#_Toc144300881)

[Security Assessment and Authorization (CA) 46](#_Toc144300882)

[CA-2 Control Assessments 46](#_Toc144300883)

[CA-3 Information Exchange (Conditional) 49](#_Toc144300884)

[CA-6 Authorization 52](#_Toc144300885)

[CA-7 Continuous Monitoring 54](#_Toc144300886)

[CA-7(4) Risk Monitoring 58](#_Toc144300887)

[CA-8 Penetration Testing 60](#_Toc144300888)

[CA-9 Internal System Connections (Conditional) 62](#_Toc144300889)

[Configuration Management (CM) 64](#_Toc144300890)

[CM-4 Impact Analysis 64](#_Toc144300891)

[CM-5 Access Restrictions for Change 67](#_Toc144300892)

[CM-6 Configuration Settings 69](#_Toc144300893)

[CM-8 System Component Inventory 72](#_Toc144300894)

[Contingency Planning (CP) 74](#_Toc144300895)

[CP-9 System Backup 74](#_Toc144300896)

[Identification and Authentication (IA) 77](#_Toc144300897)

[IA-2 (1) Multi-factor Authentication to Privileged Accounts 77](#_Toc144300898)

[IA-2(2) Multi-factor Authentication to Non-privileged Accounts 79](#_Toc144300899)

[IA-2(8) Access to Accounts — Replay Resistant 81](#_Toc144300900)

[IA-2(12) Acceptance of PIV Credentials 83](#_Toc144300901)

[IA-6 Authentication Feedback 85](#_Toc144300902)

[IA-7 Cryptographic Module Authentication 87](#_Toc144300903)

[IA-8(1) Acceptance of PIV Credentials from Other Agencies (Conditional) 89](#_Toc144300904)

[IA-8(2) Acceptance of External Authenticators (Conditional) 91](#_Toc144300905)

[Incident Response (IR) 94](#_Toc144300906)

[IR-4 Incident Handling 94](#_Toc144300907)

[IR-6 Incident Reporting 96](#_Toc144300908)

[Maintenance (MA) 98](#_Toc144300909)

[MA-2 Controlled Maintenance (Conditional) 98](#_Toc144300910)

[MA-5 Maintenance Personnel (Conditional) 101](#_Toc144300911)

[Media Protection (MP) 103](#_Toc144300912)

[MP-2 Media Access (Conditional) 103](#_Toc144300913)

[MP-6 Media Sanitization (Conditional) 105](#_Toc144300914)

[MP-7 Media Use (Conditional) 108](#_Toc144300915)

[Physical and Environmental Protection (PE) 110](#_Toc144300916)

[PE-2 Physical Access Authorizations (Conditional) 110](#_Toc144300917)

[PE-3 Physical Access Control (Conditional) 112](#_Toc144300918)

[PE-6 Monitoring Physical Access (Conditional) 115](#_Toc144300919)

[PE-8 Visitor Access Records (Conditional) 117](#_Toc144300920)

[PE-12 Emergency Lighting (Conditional) 119](#_Toc144300921)

[PE-13 Fire Protection (Conditional) 122](#_Toc144300922)

[PE-14 Environmental Controls (Conditional) 124](#_Toc144300923)

[PE-15 Water Damage Protection (Conditional) 126](#_Toc144300924)

[PE-16 Delivery and Removal (Conditional) 128](#_Toc144300925)

[Planning (PL) 130](#_Toc144300926)

[PL-2 System Security and Privacy Plans 130](#_Toc144300927)

[PL-8 Security and Privacy Architectures 133](#_Toc144300928)

[Personnel Security (PS) 136](#_Toc144300929)

[PS-3 Personnel Screening 136](#_Toc144300930)

[Risk Assessment (RA) 139](#_Toc144300931)

[RA-2 Security Categorization 139](#_Toc144300932)

[RA-3 Risk Assessment 141](#_Toc144300933)

[RA-5 Vulnerability Monitoring and Scanning 144](#_Toc144300934)

[RA-5(2) Update Vulnerabilities to Be Scanned 148](#_Toc144300935)

[RA-5(11) Public Disclosure Program 150](#_Toc144300936)

[RA-7 Risk Response 152](#_Toc144300937)

[System and Services Acquisition (SA) 154](#_Toc144300938)

[SA-9 External System Services 154](#_Toc144300939)

[SA-22 Unsupported System Components 157](#_Toc144300940)

[System and Communications Protection (SC) 159](#_Toc144300941)

[SC-5 Denial of Service Protection (Conditional) 159](#_Toc144300942)

[SC-7 Boundary Protection 161](#_Toc144300943)

[SC-8 Transmission Confidentiality and Integrity 164](#_Toc144300944)

[SC-8(1) Cryptographic Protection 167](#_Toc144300945)

[SC-12 Cryptographic Key Establishment and Management 169](#_Toc144300946)

[SC-13 Cryptographic Protection (Conditional) 172](#_Toc144300947)

[SC-28 Protection of Information at Rest 175](#_Toc144300948)

[SC-28(1) Cryptographic Protection 177](#_Toc144300949)

[System and Information Integrity (SI) 180](#_Toc144300950)

[SI-2 Flaw Remediation 180](#_Toc144300951)

[SI-3 Malicious Code Protection 182](#_Toc144300952)

[SI-4 System Monitoring 186](#_Toc144300953)

[2.0 FedRAMP LI-SaaS Assessment Results 189](#_Toc144300954)

[3.0 FedRAMP LI-SaaS [System Name] Attestation Statement 192](#_Toc144300955)

[Attestation of Policies and Procedures 192](#_Toc144300956)

[Attestation of Capabilities 227](#_Toc144300957)

# 1.0 Documented and Assessed Controls

|  |
| --- |
| ***Instructions:*** |
| *A CSP must maintain the LI-SaaS documented and assessed controls, assessment results, and control attestation sections as Section 2 to this Appendix.*  *The LI-SaaS baseline of controls is provided, in a table within Section 1, with direction for the CSP to address each control (i.e., document and assess, attest, and i4nherit etc.). A CSP is encouraged to maintain the controls as a separate document from the SSP (as the size will impact the level of effort needed to review/edit the SSP).*   * *The controls tables describe the security controls, as they are implemented, for the system. For each control, it is important to describe* ***how*** *the control is implemented and* ***from where the control originates*** *so that it is clear whose responsibility it is to implement, manage, and monitor the control.* * *Controls inheritance needs to be considered for each control – both from the perspective of the CSP inheriting controls from another CSP and inheritability of controls from the CSP to its customers (agencies or other CSPs). Please see the use case guidance, below:*   + *For controls that are inherited from another CSP, the inheriting CSP should ensure that the “Inherited” box is selected with the name of the CSP being inherited from and that the control solution description states* ***what*** *functionality is being inherited from the other CSP.*     - *Note that “-1” controls (AC-1, AU-1, SC-1, etc.) are* ***not*** *100% inherited; the inheriting CSP must describe their functions to enable inheritance; in some cases, the role may be minimal.*     - *Please remember that “inheritance” can be claimed from FedRAMP Authorized services only. If a system or service is not FedRAMP Authorized, a CSP is fully responsible for the control though another entity may perform its function.*   + *For controls defined as fully inheritable by the customer:*     - *A CSP is responsible for ensuring its implementation meets federal/FedRAMP control requirements.*     - *A third party assessment organization (3PAO) is required to validate that inherited security features can be inherited.*   + *For a control that can only be inherited, under a specific use case:*     - *The CSP must describe that use case in the SSP.*     - *The 3PAO is required to validate the control inheritability (as dictated by the use case).*   + *For controls defined as a customer responsibility, agencies are responsible for implementing, documenting, and testing the control.*   + *For shared responsibility controls:*     - *Function(s), provided by a CSP, must be clearly documented in the SSP, specifying a CSP’s responsibilities AND the responsibilities provided, or configured by, their agency customer.*     - *A 3PAO is required to test a CSP’s responsibilities.*   + *For all controls, if a CSP provides options for an agency/customer, in implementing a control, the CSP must make clear what options are compliant with federal policy.*   + *A CSP is NOT responsible for having their agency customer’s implementation of inherited controls tested.*   + *A CSP is NOT responsible for having customer-responsible controls tested.* * *Throughout the controls, policies and procedures must be explicitly referenced (title and date or version and the applicable section or paragraph numbers) so that it’s clear which document is being referred to and where, within the document, applicable details can be found.*   *Delete this instructional text from your final version of this document.* |

|  |
| --- |
| ***Instructions:*** |
| *In the sections that follow, fully describe how the information security control is implemented in the system. All controls originate from a system or from a business process. It is important to describe from where the control originates so that it is clear whose responsibility it is to implement, manage, and monitor the control. In some cases, the responsibility is shared by a CSP and their customer. Use the definitions, in the table that follows, to indicate from where each security control originates.*  *Throughout this FedRAMP Tailored LI-SaaS Framework, if documentation is referenced (e.g., policies and procedures), they must be explicitly referenced (title and date or version and the applicable section or paragraph numbers) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.*  *If there are additional CSP-specific inherited control requirements that are partially or fully inherited from the IaaS or PaaS, the “Inherited” check box must be checked, and the implementation description must simply describe what is inherited.*  *If a CSP is providing the underlying cloud infrastructure, some controls become required rather than attested to; they are noted in the above table. Agency AOs are encouraged to consider evidence, from other compliance regimes, as an approach to validating control implementation.*  *The information in each of the FedRAMP Tailored LI-SaaS Framework components must be provided, in sufficient detail about the service itself and its associated risk posture, to support federal entities in making risk-based decisions for issuing ATOs.*  *Responsible Role – Indicates the role of CSP employee(s) responsible for implementing the control.*  *Control Implementation – Descriptions of control implementations must provide sufficient detail that the implementation can be validated/assessed. This includes descriptions of what and how the security controls are implemented by the CSP (e.g., some controls are fully implemented by a CSP, and some controls have a “shared” implementation with either the underlying PaaS/IaaS and/or the customer user). Clear and concise descriptions of what is being provided by the “shared” entity must be included.*  *Assessment Plan/Procedures – Descriptions of the procedures for validating and assessing the security control implementations must be provided. If the assessor intends to incorporate assessments conducted by other entities as validation of the control, details of those assessments and determination of specific applicability must be provided.*  *Assessment Results – Descriptions of the results of the validation/assessment must be provided, including whether the required control is fully implemented or other than fully implemented. For requirements that are not fully implemented, there must be a complete description of the weakness identified, including the risk level impact to the security posture of the system (High, Moderate, or Low). Information about documentation/observations/interviews and evidence collected must be provided in support of the implementation status determination.*  *Please note: CSPs should not modify the text in the Assessment Plan/Procedures section of the control tables.*  *Below is the baseline template for the LI-SaaS Security Controls.*  *Delete this instructional text from your final version of this document.* |

The definitions in Table A-3, Control Origination and Definitions, indicate where each security control originates.

Table A-3. Control Origination and Definitions

| **Control Origination** | **Definition** | **Example** |
| --- | --- | --- |
| **Service Provider Corporate** | A control that originates from a CSP’s corporate network. | DNS from the corporate network provides address resolution services for the information system and the service offering. |
| **Service Provider System Specific** | A control specific to a particular CSP system and the control is not part of the standard corporate controls. | A unique host-based intrusion detection system (HIDs) is available on the service offering platform, but is not available on the corporate network. |
| **Service Provider Hybrid** | A control that makes use of both corporate controls and additional controls specific to a particular CSP system. | There are scans of the corporate network infrastructure; scans of databases and Web-based applications are system specific. |
| **Configured by Customer** | A control where a customer needs to apply a configuration to meet the control requirement. | User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http\* or https, etc.), entering an IP range specific to their organization are configurable by the customer. |
| **Provided by Customer** | A control where a customer needs to provide additional hardware or software to meet the control requirement. | A customer provides a SAML SSO solution to implement two-factor authentication. |
| **Shared** | A control that is managed and implemented partially by a CSP and partially by their customer. | Security awareness training must be conducted by both the CSPN and a CSP’s customer. |
| **Inherited from pre-existing FedRAMP Authorization** | A control that is inherited from another CSP system that has already received a FedRAMP authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

\**HyperText Transport Protocol (http)*

## Access Control (AC)

AC-2 Account Management

|  |
| --- |
| **AC-2 Control Requirement(s)** |
| a. Define and document the types of accounts allowed and specifically prohibited for use within the system;  b. [Excluded from FedRAMP Tailored for LI-SaaS]  c. [Excluded from FedRAMP Tailored for LI-SaaS]  d. [Excluded from FedRAMP Tailored for LI-SaaS]  1. [Excluded from FedRAMP Tailored for LI-SaaS]  2. [Excluded from FedRAMP Tailored for LI-SaaS]  3. [Excluded from FedRAMP Tailored for LI-SaaS]  e. [Excluded from FedRAMP Tailored for LI-SaaS]  f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];  g. Monitor the use of accounts;  h. Notify account managers and [Assignment: organization-defined personnel or roles] within:  1. [Assignment: organization-defined time period] when accounts are no longer required;  **AC-2 (h) (1) Additional FedRAMP Requirements and Guidance:** [twenty-four (24) hours]  2. [Assignment: organization-defined time period] when users are terminated or transferred; and  **AC-2 (h) (2) Additional FedRAMP Requirements and Guidance:** [eight (8) hours]  3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;  **AC-2 (h) (3) Additional FedRAMP Requirements and Guidance:** [eight (8) hours]  i. [Excluded from FedRAMP Tailored for LI-SaaS]  1. [Excluded from FedRAMP Tailored for LI-SaaS]  2. [Excluded from FedRAMP Tailored for LI-SaaS]  3. [Excluded from FedRAMP Tailored for LI-SaaS]  j. [Excluded from FedRAMP Tailored for LI-SaaS]  k. [Excluded from FedRAMP Tailored for LI-SaaS]  l. [Excluded from FedRAMP Tailored for LI-SaaS] |
| **AC-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AC-2 What is the solution and how is it implemented?** |
| Description of how AC-2 is implemented,  Customer Responsibilities |
| **AC-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:  a. (1) account types allowed for use within the system are defined and documented  (2) account types specifically prohibited for use within the system are defined and documented;  f. (1) accounts are created in accordance with policy and procedure  (2) accounts are enabled in accordance with policy and procedure  (3) accounts are modified in accordance with policy and procedure  (4) accounts are disabled in accordance with policy and procedure  (5) accounts are removed in accordance with policy and procedure  g. the use of accounts is monitored;  h. (1) account managers and are notified within twenty-four (24) hours when accounts are no longer required;  (2) account managers are notified within eight (8) hours when users are terminated or transferred.  (3) account managers are notified within eight (8) hours when system usage or the need-to-know changes for an individual; |
| **Assessment Procedures:**   * **EXAMINE:** Access control policy; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of active system accounts along with the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; information system monitoring records; information system audit records; other relevant documents or records. * **INTERVIEW:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities. * **TEST:** Organizational processes for account management on the information system; automated mechanisms for implementing account management. |
| **AC-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AC-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

AC-3 Access Enforcement

|  |
| --- |
| **AC-3 Control Requirement(s)** |
| Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. |
| **AC-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AC-3 What is the solution and how is it implemented?** |
| Description of how AC-3 is implemented,  Customer Responsibilities |
| **AC-3 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if approved authorizations for logical access to information and system resources are enforced in accordance with applicable access control policies. |
| **Assessment Procedures:**   * **EXAMINE:** Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of approved authorizations (user privileges) system audit records; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers. * **TEST:** Mechanisms implementing access control policy. |
| **AC-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AC-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

AC-7 Unsuccessful Logon Attempts

|  |
| --- |
| **AC-7 Control Requirement(s)** |
| a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid log-on attempts by a user during a [Assignment: organization-defined time period]; and  b. Automatically [Assignment: lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.  **AC-7 (a and b) Requirement: In alignment with NIST SP 800-63B** |
| **AC-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AC-7 What is the solution and how is it implemented?** |
| Description of how AC-7 is implemented,  Customer Responsibilities |
| **AC-7 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * a limit of number of consecutive invalid logon attempts by a user during time period as specified in NIST SP 800 63B is enforced; * automatically lock the account or node for a time period specified in NIST SP 800 63B when the maximum number of unsuccessful attempts is exceeded. |
| **Assessment Procedures:**   * **EXAMINE:** Access control policy; procedures addressing unsuccessful logon attempts; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with information security responsibilities; system developers; system/network administrators. * **TEST:** Mechanisms implementing access control policy for unsuccessful logon attempts. |
| **AC-7 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AC-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

AC-17 Remote Access

|  |
| --- |
| **AC-17 Control Requirement(s)** |
| a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and  b. Authorize each type of remote access to the system prior to allowing such connections. |
| **AC-17 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AC-17 What is the solution and how is it implemented?** |
| Description of how AC-17 is implemented,  Customer Responsibilities |
| **AC-17 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if each type of remote access to the system is authorized prior to allowing such connections. |
| **Assessment Procedures:**   * **EXAMINE:** Access control policy; procedures addressing remote access implementation and usage (including restrictions) configuration management plan; system configuration settings and associated documentation; remote access authorizations; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for managing remote access connections; system/network administrators; organizational personnel with information security responsibilities. * **TEST:** Remote access management capability for the system. |
| **AC-17 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AC-17 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

AC-22 Publicly Accessible Content

|  |
| --- |
| **AC-22 Control Requirement(s)** |
| a. Designate individuals authorized to make information publicly accessible;  b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;  c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and  d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.  **AC-22 (d) Additional FedRAMP Requirements and Guidance:** [at least quarterly] |
| **AC-22 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AC-22 What is the solution and how is it implemented?** |
| Description of how AC-22 is implemented,  Customer Responsibilities |
| **AC-22 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * designated individuals are authorized to make information publicly accessible; * authorized individuals are trained to ensure that publicly accessible information does not contain non-public information; and * the proposed content of information is reviewed prior to posting onto the publicly accessible system to ensure that non-public information is not included. |
| **Assessment Procedures:**   * **EXAMINE:** Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to non-public information on public websites; system audit logs; security awareness training records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for managing publicly accessible information posted on organizational systems; organizational personnel with information security responsibilities. * **TEST:** Mechanisms implementing management of publicly accessible content. |
| **AC-22 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AC-22 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Audit and Accountability (AU)

AU-3 Content of Audit Records

|  |
| --- |
| **AU-3 Control Requirement(s)** |
| Ensure that audit records contain information that establishes the following:  a. What type of event occurred;  b. When the event occurred;  c. Where the event occurred;  d. Source of the event;  e. Outcome of the event; and  f. Identity of any individuals, subjects, or objects/entities associated with the event. |
| **AU-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AU-3 What is the solution and how is it implemented?** |
| Description of how AU-3 is implemented,  Customer Responsibilities |
| **AU-3 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * audit records contain information that establishes what type of event occurred; * plans are reviewed at least annually; * audit records contain information that establishes where the event occurred; * audit records contain information that establishes the source of the event; * audit records contain information that establishes the outcome of the event; and * audit records contain information that establishes the identity of any individuals, subjects, or objects/entities associated with the event. |
| **Assessment Procedures:**   * **EXAMINE:** Audit and accountability policy; system security plan; privacy plan; procedures addressing content of audit records; system design documentation; system configuration settings and associated documentation; list of organization-defined auditable events; system audit records; system incident reports; other relevant documents or records. * **INTERVIEW:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators. * **TEST:** Mechanisms implementing system auditing of auditable events. |
| **AU-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AU-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

AU-5 Response to Audit Logging Process Failures

|  |
| --- |
| **AU-5 Control Requirement(s)** |
| a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined personnel or roles] in the event of an audit logging process failure; and [Assignment: organization-defined time period]  b. Take the following additional actions: [Assignment: organization-defined additional actions].  **AU-5 (b) Additional FedRAMP Requirements and Guidance:** [overwrite oldest record] |
| **AU-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AU-5 What is the solution and how is it implemented?** |
| Description of how AU-5 is implemented,  Customer Responsibilities |
| **AU-5 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * personnel or roles are alerted in the event of an audit logging process failure within time period; and * additional actions to be taken in the event of an audit logging process failure are defined. |
| **Assessment Procedures:**   * **EXAMINE:** Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; system audit records; other relevant documents or records. * **INTERVIEW:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers. * **TEST:** Mechanisms implementing system response to audit processing failures. |
| **AU-5 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AU-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

AU-6 Audit Record Review, Analysis, and Reporting

|  |
| --- |
| **AU-6 Control Requirement(s)** |
| a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined frequency] and the potential impact of the inappropriate or unusual activity; [Assignment: organization-defined inappropriate or unusual activity]  **AU-6 (a)-1 Additional FedRAMP Requirements and Guidance:** [at least weekly]  **AU-6 (a)-1 Additional FedRAMP Requirements and Guidance:** Coordination between service provider and consumer shall be documented and accepted by the JAB/AO. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.  b. Report findings to [Assignment: organization-defined personnel or roles]; and  c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. |
| **AU-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **AU-6 What is the solution and how is it implemented?** |
| Description of how AU-6 is implemented,  Customer Responsibilities |
| **AU-6 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * system audit records are reviewed and analyzed at least weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity; * findings are reported to personnel or roles; and * the level of audit record review, analysis, and reporting within the system is adjusted when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. |
| **Assessment Procedures:**   * **EXAMINE:** Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records. * **INTERVIEW:** Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities. |
| **AU-6 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **AU-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Security Assessment and Authorization (CA)

CA-2 Control Assessments

|  |
| --- |
| **CA-2 Control Requirement(s)** |
| a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;  b. Develop a control assessment plan that describes the scope of the assessment including:  1. Controls and control enhancements under assessment;  2. Assessment procedures to be used to determine control effectiveness; and  3. Assessment environment, assessment team, and assessment roles and responsibilities;  c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;  d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy  **CA-2 (d) Additional FedRAMP Requirements and Guidance:** [at least annually]  e. Produce a control assessment report that document the results of the assessment; and  f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].  **CA-2 (f) Additional FedRAMP Requirements and Guidance:** [individuals or roles to include FedRAMP PMO]  **CA-2 Additional FedRAMP Requirements and Guidance:** Reference FedRAMP Annual Assessment Guidance. |
| **CA-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CA-2 What is the solution and how is it implemented?** |
| Description of how CA-2 is implemented,  Customer Responsibilities |
| **CA-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * an appropriate assessor or assessment team is selected for the type of assessment to be conducted; * the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; * a control assessment report is produced that documents the results of the assessment; and * the results of the control assessment are provided individuals or roles to include FedRAMP PMO. |
| **Assessment Procedures:**   * **EXAMINE:** Assessment, authorization, and monitoring policy; procedures addressing assessment planning; procedures addressing control assessments; control assessment plan; control assessment report; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities. * **TEST:** Mechanisms supporting control assessment, control assessment plan development, and/or control assessment reporting. |
| **CA-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CA-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CA-3 Information Exchange (Conditional)

|  |
| --- |
| **CA-3 Control Requirement(s)** |
| a. Approve and manage the exchange of information between the system and other systems using [Assignment: interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements];  b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and  c. Review and update the agreements [Assignment: organization-defined frequency].  **CA-3 (c) Additional FedRAMP Requirements and Guidance:** [at least annually and on input from JAB/AO] |
| **CA-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CA-3 What is the solution and how is it implemented?** |
| Description of how CA-3 is implemented,  Customer Responsibilities |
| **CA-3 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * at the exchange of information between the system and other systems is approved and managed using interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; non-disclosure agreements; and * agreements are reviewed and updated at least annually and on input from JAB/AO. |
| **Assessment Procedures:**   * **EXAMINE:** Access control policy; procedures addressing system connections; system and communications protection policy; system interconnection security agreements; information exchange security agreements; memoranda of understanding or agreements; service level agreements; non-disclosure agreements; system design documentation; enterprise architecture; system architecture; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for developing, implementing, or approving system interconnection agreements; organizational personnel with information security and privacy responsibilities; personnel managing the system(s) to which the interconnection security agreement applies. |
| **CA-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CA-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CA-6 Authorization

|  |
| --- |
| **CA-6 Control Requirement(s)** |
| a. Assign a senior official as the authorizing official for the system;  b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;  c. Ensure that the authorizing official for the system, before commencing operations:  1. Accepts the use of common controls inherited by the system; and  2. Authorizes the system to operate;  d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;  e. Update the authorizations [Assignment: organization-defined frequency].  **CA-6 (e) Additional FedRAMP Requirements and Guidance:** [in accordance with OMB A-130 requirements or when a significant change occurs]  **CA-6 (e) Additional FedRAMP Requirements and Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F and according to FedRAMP Significant Change Policies and Procedures. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO. |
| **CA-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CA-6 What is the solution and how is it implemented?** |
| Description of how CA-6 is implemented,  Customer Responsibilities |
| **CA-6 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * a senior official is assigned as the authorizing official for the system; * a senior official is assigned as the authorizing official for common controls available for inheritance by organizational systems; * the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; and * the authorizations are updated in accordance with OMB A-130 requirements or when a significant change occurs. |
| **Assessment Procedures:**   * **EXAMINE:** Assessment, authorization, and monitoring policy; procedures addressing authorization; system security plan, privacy plan, assessment report, plan of action and milestones; authorization statement; other relevant documents or records. * **INTERVIEW:** Organizational personnel with authorization responsibilities; organizational personnel with information security and privacy responsibilities. * **TEST:** Mechanisms that facilitate authorizations and updates. |
| **CA-6 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CA-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CA-7 Continuous Monitoring

|  |
| --- |
| **CA-7 Control Requirement(s)** |
| Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:  a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];  b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;  c. Ongoing control assessments in accordance with the continuous monitoring strategy;  d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;  e. Correlation and analysis of information generated by control assessments and monitoring;  f. Response actions to address results of the analysis of control assessment and monitoring information; and  g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].  **CA-7 (g)-1 Additional FedRAMP Requirements and Guidance:** [to include JAB/AO]  **CA-7 Additional FedRAMP Requirements and Guidance:** Operating System, Database, Web Application, Container, and Service Configuration Scans: at least monthly. All scans performed by Independent Assessor: at least annually.  **CA-7 Requirement:** CSOs with more than one agency ATO must implement a collaborative Continuous Monitoring (ConMon) approach described in the FedRAMP Guide for Multi-Agency Continuous Monitoring. This requirement applies to CSOs authorized via the Agency path as each agency customer is responsible for performing ConMon oversight. It does not apply to CSOs authorized via the JAB path because the JAB performs ConMon oversight.  **CA-7 Guidance:** FedRAMP does not provide a template for the Continuous Monitoring Plan. CSPs should reference the FedRAMP Continuous Monitoring Strategy Guide when developing the Continuous Monitoring Plan. |
| **CA-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CA-7 What is the solution and how is it implemented?** |
| Description of how CA-7 is implemented,  Customer Responsibilities |
| **CA-7 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * a system-level continuous monitoring strategy is developed; * system-level continuous monitoring is implemented in accordance with the organization-level continuous monitoring strategy; * system-level continuous monitoring includes establishment of the following system-level metrics to be monitored: system-level metrics; * system-level continuous monitoring includes ongoing control assessments in accordance with the continuous monitoring strategy; * system-level continuous monitoring includes ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; * system-level continuous monitoring includes correlation and analysis of information generated by control assessments and monitoring; and * system-level continuous monitoring includes response actions to address the results of the analysis of control assessment and monitoring information. |
| **Assessment Procedures:**   * **EXAMINE:** Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls; procedures addressing configuration management; control assessment report; plan of action and milestones; system monitoring records; configuration management records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators. * **TEST:** Mechanisms implementing continuous monitoring; mechanisms supporting response actions to address assessment and monitoring results; mechanisms supporting security and privacy status reporting. |
| **CA-7 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CA-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CA-7(4) Risk Monitoring

|  |
| --- |
| **CA-7(4) Control Requirement(s)** |
| Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:  (a) Effectiveness monitoring;  (b) Compliance monitoring; and  (c) Change monitoring. |
| **CA-7(4) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CA-7(4) What is the solution and how is it implemented?** |
| Description of how CA-7(4) is implemented,  Customer Responsibilities |
| **CA-7(4) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * risk monitoring is an integral part of the continuous monitoring strategy; * effectiveness monitoring is included in risk monitoring; * compliance monitoring is included in risk monitoring; and * change monitoring is included in risk monitoring. |
| **Assessment Procedures:**   * **EXAMINE:** Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls; assessment report; plan of action and milestones; system monitoring records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities. * **TEST:** Mechanisms supporting risk monitoring. |
| **CA-7(4) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CA-7(4) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CA-8 Penetration Testing

|  |
| --- |
| **CA-8 Control Requirement(s)** |
| Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].  **CA-8-1 Additional FedRAMP Requirements and Guidance:** [at least annually]  **CA-8 Additional FedRAMP Requirements and Guidance:** Scope can be limited to public facing applications in alignment with M-22-09. Reference the FedRAMP Penetration Test Guidance. |
| **CA-8 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CA-8 What is the solution and how is it implemented?** |
| Description of how CA-8 is implemented,  Customer Responsibilities |
| **CA-8 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if penetration testing is conducted at least annually on system(s) or system components. |
| **Assessment Procedures:**   * **EXAMINE:** Assessment, authorization, and monitoring policy; procedures addressing penetration testing; assessment plan; penetration test report; assessment report; assessment evidence; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators. * **TEST:** Mechanisms supporting penetration testing. |
| **CA-8 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CA-8 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CA-9 Internal System Connections (Conditional)

|  |
| --- |
| **CA-9 Control Requirement(s)** |
| a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;  b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;  c. Terminate internal system connections after [Assignment: organization-defined conditions]; and  d. Review [Assignment: organization-defined frequency] the continued need for each internal connection. |
| **CA-9 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CA-9 What is the solution and how is it implemented?** |
| Description of how CA-9 is implemented,  Customer Responsibilities |
| **CA-9 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * internal connections of system components to the system are authorized; * internal system connections are terminated after conditions; and * the continued need for each internal connection is reviewed frequency. |
| **Assessment Procedures:**   * **EXAMINE:** Assessment, authorization, and monitoring policy; access control policy; procedures addressing system connections; system and communications protection policy; system design documentation; system configuration settings and associated documentation; list of components or classes of components authorized as internal system connections; assessment report; system audit records; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for developing, implementing, or authorizing internal system connections; organizational personnel with information security and privacy responsibilities. * **TEST:** Mechanisms supporting internal system connections. |
| **CA-9 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CA-9 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Configuration Management (CM)

CM-4 Impact Analysis

|  |
| --- |
| **CM-4 Control Requirement(s)** |
| Analyze changes to the system to determine potential security and privacy impacts prior to change implementation. |
| **CM-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CM-4 What is the solution and how is it implemented?** |
| Description of how CM-4 is implemented,  Customer Responsibilities |
| **CM-4 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * changes to the system are analyzed to determine potential security impacts prior to change implementation; and * changes to the system are analyzed to determine potential privacy impacts prior to change implementation. |
| **Assessment Procedures:**   * **EXAMINE:** Configuration management policy; procedures addressing security impact analyses for changes to the system; procedures addressing privacy impact analyses for changes to the system; configuration management plan; security impact analysis documentation; privacy impact analysis documentation; privacy impact assessment; privacy risk assessment documentation, system design documentation; analysis tools and associated outputs; change control records; system audit records; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibility for conducting security impact analyses; organizational personnel with responsibility for conducting privacy impact analyses; organizational personnel with information security and privacy responsibilities; system developer; system/network administrators; members of change control board or similar. * **TEST:** Organizational processes for security impact analyses; organizational processes for privacy impact analyses. |
| **CM-4 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CM-4 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CM-5 Access Restrictions for Change

|  |
| --- |
| **CM-5 Control Requirement(s)** |
| Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system. |
| **CM-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CM-5 What is the solution and how is it implemented?** |
| Description of how CM-5 is implemented,  Customer Responsibilities |
| **CM-5 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * physical access restrictions associated with changes to the system are defined and documented; * physical access restrictions associated with changes to the system are approved; * physical access restrictions associated with changes to the system are enforced; * logical access restrictions associated with changes to the system are defined and documented; * logical access restrictions associated with changes to the system are approved; and * logical access restrictions associated with changes to the system are enforced. |
| **Assessment Procedures:**   * **EXAMINE:** Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; logical access approvals; physical access approvals; access credentials; change control records; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators. * **TEST:** Organizational processes for managing access restrictions to change; mechanisms supporting, implementing, or enforcing access restrictions associated with changes to the system. |
| **CM-5 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CM-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CM-6 Configuration Settings

|  |
| --- |
| **CM-6 Control Requirement(s)** |
| a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];  b. Implement the configuration settings;  c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and  d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.  **CM-6 (a)-1 Additional FedRAMP Requirements and Guidance:** The service provider shall use the DoD STIGs or Center for Internet Security guidelines to establish configuration settings;  **CM-6 (a)-2 Additional FedRAMP Requirements and Guidance:** The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).  **CM-6 Additional FedRAMP Requirements and Guidance:**  Compliance checks are used to evaluate configuration settings and provide general insight into the overall effectiveness of configuration management activities. CSPs and 3PAOs typically combine compliance check findings into a single CM-6 finding, which is acceptable. However, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a per-control basis, where risks exist. Therefore, 3PAOs must also analyze compliance check findings as part of the controls assessment. Where a direct mapping exists, the 3PAO must document additional findings per control in the corresponding SAR Risk Exposure Table (RET), which are then documented in the CSP’s Plan of Action and Milestones (POA&M). This will likely result in the details of individual control findings overlapping with those in the combined CM-6 finding, which is acceptable.  During monthly continuous monitoring, new findings from CSP compliance checks may be combined into a single CM-6 POA&M item. CSPs are not required to map the findings to specific controls because controls are only assessed during initial assessments, annual assessments, and significant change requests. |
| **CM-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CM-6 What is the solution and how is it implemented?** |
| Description of how CM-6 is implemented,  Customer Responsibilities |
| **CM-6 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * configuration settings that reflect the most restrictive mode consistent with operational requirements are established and documented for components employed within the system using common secure configurations; and * the configuration settings documented in CM-06a are implemented. |
| **Assessment Procedures:**   * **EXAMINE:** Configuration management policy; procedures addressing configuration settings for the system; configuration management plan; system design documentation; system configuration settings and associated documentation; common secure configuration checklists; system component inventory; evidence supporting approved deviations from established configuration settings; change control records; system data processing and retention permissions; system audit records; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with security configuration management responsibilities; organizational personnel with privacy configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators. * **TEST:** Organizational processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings. |
| **CM-6 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CM-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

CM-8 System Component Inventory

|  |
| --- |
| **CM-8 Control Requirement(s)** |
| a. Develop and document an inventory of system components that:  1. Accurately reflects the system;  2. Includes all components within the system;  3. Does not include duplicate accounting of components or components assigned to any other system;  4. Is at the level of granularity deemed necessary for tracking and reporting; and  5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and  b. Review and update the system component inventory [Assignment: organization-defined frequency].  **CM-8 (b) Additional FedRAMP Requirements and Guidance:** [at least monthly]  **CM-8 Additional FedRAMP Requirements and Guidance:** must be provided at least monthly or when there is a change. |
| **CM-8 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CM-8 What is the solution and how is it implemented?** |
| Description of how CM-8 is implemented,  Customer Responsibilities |
| **CM-8 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if the system component inventory is reviewed and updated at least monthly. |
| **Assessment Procedures:**   * **EXAMINE:** Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system design documentation; system component inventory; inventory reviews and update records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with component inventory management responsibilities; organizational personnel with information security responsibilities; system/network administrators. * **TEST:** Organizational processes for managing the system component inventory; mechanisms supporting and/or implementing system component inventory. |
| **CM-8 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CM-8 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Contingency Planning (CP)

CP-9 System Backup

|  |
| --- |
| **CP-9 Control Requirement(s)** |
| a. Conduct backups of user-level information contained in [Assignment: organization-defined system components]; [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]  **CP-9 (a)-2 Additional FedRAMP Requirements and Guidance:** [daily incremental; weekly full]  **CP-9 (a) Additional FedRAMP Requirements and Guidance:** 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.  b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];  **CP-9 (b) Additional FedRAMP Requirements and Guidance:** [daily incremental; weekly full]  **CP-9 (b) Additional FedRAMP Requirements and Guidance:** 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.  c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and  **CP-9 (c) Additional FedRAMP Requirements and Guidance:** [daily incremental; weekly full]  **CP-9 (c) Additional FedRAMP Requirements and Guidance**: 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.  d. Protect the confidentiality, integrity, and availability of backup information.  **CP-9 Requirement:** The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check. |
| **CP-9 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **CP-9 What is the solution and how is it implemented?** |
| Description of how CP-9 is implemented,  Customer Responsibilities |
| **CP-9 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * backups of user-level information contained in system components are conducted daily incremental; weekly full; * backups of system-level information contained in the system are conducted daily incremental; weekly full; and * backups of system documentation, including security- and privacy-related documentation are conducted daily incremental; weekly full. |
| **Assessment Procedures:**   * **EXAMINE:** Contingency planning policy; procedures addressing system backup; contingency plan; backup storage location(s)system backup logs or records; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system backup responsibilities; organizational personnel with information security and privacy responsibilities. * **TEST:** Organizational processes for conducting system backups; mechanisms supporting and/or implementing system backups. |
| **CP-9 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **CP-9 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Identification and Authentication (IA)

IA-2 (1) Multi-factor Authentication to Privileged Accounts

|  |
| --- |
| **IA-2(1) Control Requirement(s)** |
| Implement multi-factor authentication for access to privileged accounts.   * **IA-2 (1)** **Additional FedRAMP Requirements and Guidance:** According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL). * **IA-2 (1)** **Additional FedRAMP Requirements and Guidance:** Multi-factor authentication must be phishing-resistant. * **IA-2 (1)** **Additional FedRAMP Requirements and Guidance:** Multi-factor authentication to subsequent components in the same user domain is not required. |
| **IA-2(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-2(1) What is the solution and how is it implemented?** |
| Description of how IA-2(1) is implemented,  Customer Responsibilities |
| **IA-2(1) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine ifmulti-factor authentication is implemented for access to privileged accounts. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. * **TEST:** Mechanisms supporting and/or implementing a multi-factor authentication capability. |
| **IA-2(1) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-2(1) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IA-2(2) Multi-factor Authentication to Non-privileged Accounts

|  |
| --- |
| **IA-2(2) Control Requirement(s)** |
| Implement multi-factor authentication for access to non-privileged accounts.   * **IA-2 (2)** **Additional FedRAMP Requirements and Guidance:** According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL). * **IA-2 (2)** **Additional FedRAMP Requirements and Guidance:** Multi-factor authentication must be phishing-resistant. * **IA-2 (2)** **Additional FedRAMP Requirements and Guidance:** Multi-factor authentication to subsequent components in the same user domain is not required. |
| **IA-2(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-2(2) What is the solution and how is it implemented?** |
| Description of how IA-2(2) is implemented,  Customer Responsibilities |
| **IA-2(2) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if multi-factor authentication is implemented for access to non-privileged accounts. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. * **TEST:** Mechanisms supporting and/or implementing a multi-factor authentication capability. |
| **IA-2(2) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-2(2) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IA-2(8) Access to Accounts — Replay Resistant

|  |
| --- |
| **IA-2(8) Control Requirement(s)** |
| Implement replay-resistant authentication mechanisms for access to [Assignment: privileged accounts; non-privileged accounts]. |
| **IA-2(8) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-2(8) What is the solution and how is it implemented?** |
| Description of how IA-2(8) is implemented,  Customer Responsibilities |
| **IA-2(8) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if replay-resistant authentication mechanisms for access to user accounts are implemented. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of privileged system accounts; other relevant documents or records. * **INTERVEIW:** Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. * **TEST:** Mechanisms supporting and/or implementing identification and authentication capabilities; Mechanisms supporting and/or implementing replay resistant authentication mechanisms. |
| **IA-2(8) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-2(8) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IA-2(12) Acceptance of PIV Credentials

|  |
| --- |
| **IA-2(12) Control Requirement(s)** |
| Accept and electronically verify Personal Identity Verification-compliant credentials.   * **IA-2 (12)** **Additional FedRAMP Requirements and Guidance:** Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12. |
| **IA-2(12) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-2(12) What is the solution and how is it implemented?** |
| Description of how IA-2(12) is implemented,  Customer Responsibilities |
| **IA-2(12) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine ifPersonal Identity Verification-compliant credentials are accepted and electronically verified. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation system audit records; PIV verification records; evidence of PIV credentials; PIV credential authorizations; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system responsibilities; operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with informational security responsibilities; system/network administrators; system developers. * **TEST:** Mechanisms supporting and/or implementing acceptance and verification of PIV credentials. |
| **IA-2(12) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-2(12) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IA-6 Authentication Feedback

|  |
| --- |
| **IA-6 Control Requirement(s)** |
| Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals. |
| **IA-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-6 What is the solution and how is it implemented?** |
| Description of how IA-6 is implemented,  Customer Responsibilities |
| **IA-6 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if the feedback of authentication information is obscured during the authentication process to protect the information from possible exploitation and use by unauthorized individuals. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; system security plan; procedures addressing authenticator feedback; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records. * **INTERVIEW:** Organizational personnel with information security responsibilities; system/network administrators; system developers. * **TEST:** Mechanisms supporting and/or implementing the obscuring of feedback of authentication information during authentication. |
| **IA-6 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IA-7 Cryptographic Module Authentication

|  |
| --- |
| **IA-7 Control Requirement(s)** |
| Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication. |
| **IA-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-7 What is the solution and how is it implemented?** |
| Description of how IA-7 is implemented,  Customer Responsibilities |
| **IA-7 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if mechanisms for authentication to a cryptographic module are implemented that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; system security plan; procedures addressing cryptographic module authentication; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibility for cryptographic module authentication; organizational personnel with information security responsibilities; system/network administrators; system developers. * **TEST:** Mechanisms supporting and/or implementing cryptographic module authentication. |
| **IA-7 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IA-8(1) Acceptance of PIV Credentials from Other Agencies (Conditional)

|  |
| --- |
| **IA-8(1) Control Requirement(s)** |
| Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies. |
| **IA-8(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-8(1) What is the solution and how is it implemented?** |
| Description of how IA-8(1) is implemented,  Customer Responsibilities |
| **IA-8(1) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * Personal Identity Verification on-compliant credentials from other federal agencies are accepted;and * Personal Identity Verification on-compliant credentials from other federal agencies are electronically verified. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; system security plan; procedures addressing user Identification and authentication; system design documentation; system configuration settings; and associated documentation; system audit records; PIV verification records; evidence of PIV credentials; PIV credential authorizations; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; system developers; organizational personnel with account management responsibilities. * **TEST:** Mechanisms supporting and/or implementing Identification and authentication capabilities; mechanisms that accept and verify PIV credentials. |
| **IA-8(1) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-8(1) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IA-8(2) Acceptance of External Authenticators (Conditional)

|  |
| --- |
| **IA-8(2) Control Requirement(s)** |
| (a) Accept only external authenticators that are NIST-compliant; and  (b) Document and maintain a list of accepted external authenticators. |
| **IA-8(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IA-8(2) What is the solution and how is it implemented?** |
| Description of how IA-8(2) is implemented,  Customer Responsibilities |
| **IA-8(2) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * only external authenticators that are NIST-compliant are accepted;   1. a list of accepted external authenticators is documented   2. a list of accepted external authenticators is maintained. |
| **Assessment Procedures:**   * **EXAMINE:** Identification and authentication policy; system security plan; procedures addressing user Identification and authentication; system design documentation; system configuration settings; and associated documentation; system audit records; list of third-party credentialing products, components, or services procured and implemented by organization; third-party credential verification records; evidence of third-party credentials; third-party credential authorizations; other relevant documents or records. * **INTERVIEW** Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; system developers; organizational personnel with account management responsibilities. * **TEST:** Mechanisms supporting and/or implementing Identification and authentication capabilities; mechanisms that accept external credentials. |
| **IA-8(2) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IA-8(2) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Incident Response (IR)

IR-4 Incident Handling

|  |
| --- |
| **IR-4 Control Requirement(s)** |
| a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;  b. Coordinate incident handling activities with contingency planning activities;  c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and  d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.   * IR-4 **Additional FedRAMP Requirements and Guidance:** The FISMA definition of "incident" shall be used: "An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." * IR-4 **Additional FedRAMP Requirements and Guidance:** 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-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IR-4 What is the solution and how is it implemented?** |
| Description of how IR-4 is implemented,  Customer Responsibilities |
| **IR-4 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if incident handling activities are coordinated with contingency planning activities. |
| **Assessment Procedures:**   * **EXAMINE:** Incident response policy; contingency planning policy; procedures addressing incident handling; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities; organizational personnel with information security and privacy responsibilities. * **TEST:** Incident handling capability for the organization. |
| **IR-4 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IR-4 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

IR-6 Incident Reporting

|  |
| --- |
| **IR-6 Control Requirement(s)** |
| a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and  **IR-6 (a) Additional FedRAMP Requirements and Guidance:** [US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]  b. Report incident information to [Assignment: organization-defined authorities].  **IR-6** **Additional FedRAMP Requirements and Guidance:** Reports security incident information according to FedRAMP Incident Communications Procedure. |
| **IR-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **IR-6 What is the solution and how is it implemented?** |
| Description of how IR-6 is implemented,  Customer Responsibilities |
| **IR-6 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * personnel is/are required to report suspected incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended); * incident information is reported to authorities. |
| **Assessment Procedures:**   * **EXAMINE:** Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with incident reporting responsibilities; organizational personnel with information security and privacy responsibilities; personnel who have/should have reported incidents; personnel (authorities) to whom incident information is to be reported; system users. * **TEST:** Organizational processes for incident reporting; mechanisms supporting and/or implementing incident reporting. |
| **IR-6 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **IR-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Maintenance (MA)

MA-2 Controlled Maintenance (Conditional)

|  |
| --- |
| **MA-2 Control Requirement(s)** |
| a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;  b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;  c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;  d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];  e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and  f. Include the following information in organizational maintenance records: [Assignment: organization-defined information]. |
| **MA-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **MA-2 What is the solution and how is it implemented?** |
| Description of how MA-2 is implemented,  Customer Responsibilities |
| **MA-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * personnel or roles is/are required to explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; * equipment is sanitized to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement; * all potentially impacted controls are checked to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and * information is included in organizational maintenance records. |
| **Assessment Procedures:**   * **EXAMINE:** Maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators. * **TEST:** Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the system; organizational processes for sanitizing system components; mechanisms supporting and/or implementing controlled maintenance; mechanisms implementing the sanitization of system components. |
| **MA-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **MA-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

MA-5 Maintenance Personnel (Conditional)

|  |
| --- |
| **MA-5 Control Requirement(s)** |
| a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;  b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and  c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. |
| **MA-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **MA-5 What is the solution and how is it implemented?** |
| Description of how MA-5 is implemented,  Customer Responsibilities |
| **MA-5 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * non-escorted personnel performing maintenance on the system possess the required access authorizations; and * organizational personnel with required access authorizations and technical competence is/are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations. |
| **Assessment Procedures:**   * **EXAMINE:** Maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities. * **TEST:** Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting and/or implementing authorization of maintenance personnel. |
| **MA-5 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **MA-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Media Protection (MP)

MP-2 Media Access (Conditional)

|  |
| --- |
| **MP-2 Control Requirement(s)** |
| Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles]. |
| **MP-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **MP-2 What is the solution and how is it implemented?** |
| Description of how MP-2 is implemented,  Customer Responsibilities |
| **MP-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * access to types of digital media is restricted to organizationally defined personnel or roles; and * access to types of non-digital media is restricted to organizationally defined personnel or roles. |
| **Assessment Procedures:**   * **EXAMINE:** System media protection policy; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system media protection responsibilities; organizational personnel with information security responsibilities; system/network administrators. * **TEST:** Organizational processes for restricting information media; mechanisms supporting and/or implementing media access restrictions. |
| **MP-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **MP-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

MP-6 Media Sanitization (Conditional)

|  |
| --- |
| **MP-6 Control Requirement(s)** |
| a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and  **MP-6 (a)-2 Additional FedRAMP Requirements and Guidance:** [techniques and procedures IAW NIST SP 800-88 Section 4: Reuse and Disposal of Storage Media and Hardware]  b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. |
| **MP-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **MP-6 What is the solution and how is it implemented?** |
| Description of how MP-6 is implemented,  Customer Responsibilities |
| **MP-6 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information are employed. |
| **Assessment Procedures:**   * **EXAMINE:** System media protection policy; procedures addressing media sanitization and disposal; applicable federal standards and policies addressing media sanitization policy; media sanitization records; system audit records; system design documentation; records retention and disposition policy; records retention and disposition procedures; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with media sanitization responsibilities; organizational personnel with records retention and disposition responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators. * **TEST:** Organizational processes for media sanitization; mechanisms supporting and/or implementing media sanitization. |
| **MP-6 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **MP-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

MP-7 Media Use (Conditional)

|  |
| --- |
| **MP-7 Control Requirement(s)** |
| a. [Assignment: Restrict; Prohibit] the use of [Assignment: Restrict; Prohibit] on [Assignment: Restrict; Prohibit] using [Assignment: organization-defined types of system media]; and  b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner. |
| **MP-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **MP-7 What is the solution and how is it implemented?** |
| Description of how MP-7 is implemented,  Customer Responsibilities |
| **MP-7 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * the use of types of system media is restricted; prohibited on systems or system components using controls; and * the use of portable storage devices in organizational systems is prohibited when such devices have no identifiable owner. |
| **Assessment Procedures:**   * **EXAMINE:** System media protection policy; system use policy; procedures addressing media usage restrictions; rules of behavior; system design documentation; system configuration settings and associated documentation; audit records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system media use responsibilities; organizational personnel with information security responsibilities; system/network administrators. * **TEST:** Organizational processes for media use; mechanisms restricting or prohibiting the use of system media on systems or system components. |
| **MP-7 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **MP-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Physical and Environmental Protection (PE)

PE-2 Physical Access Authorizations (Conditional)

|  |
| --- |
| **PE-2 Control Requirement(s)** |
| a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;  b. Issue authorization credentials for facility access;  c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and  **PE-2 (c) Additional FedRAMP Requirements and Guidance:** [at least annually]  d. Remove individuals from the facility access list when access is no longer required. |
| **PE-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-2 What is the solution and how is it implemented?** |
| Description of how PE-2 is implemented,  Customer Responsibilities |
| **PE-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * authorization credentials are issued for facility access; * the access list detailing authorized facility access by individuals is reviewed the access list detailing authorized facility access by individuals is reviewed; and * individuals are removed from the facility access list when access is no longer required. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to system facility; organizational personnel with information security responsibilities. * **TEST:** Organizational processes for physical access authorizations; mechanisms supporting and/or implementing physical access authorizations. |
| **PE-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-3 Physical Access Control (Conditional)

|  |
| --- |
| **PE-3 Control Requirement(s)** |
| a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:  1. Verifying individual access authorizations before granting access to the facility; and  2. Controlling ingress and egress to the facility using [Assignment: guards];  **PE-3 (a)-2 Additional FedRAMP Requirements and Guidance:** [CSP defined physical access control systems/devices AND guards]  b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];  c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];  d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity];  **PE-3 (d) Additional FedRAMP Requirements and Guidance:** [in all circumstances within restricted access area where the information system resides]  e. Secure keys, combinations, and other physical access devices;  f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and  **PE-3 (f)-2 Additional FedRAMP Requirements and Guidance:** [at least annually]  g. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.  **PE-3 (g) Additional FedRAMP Requirements and Guidance:** [at least annually] |
| **PE-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-3 What is the solution and how is it implemented?** |
| Description of how PE-3 is implemented,  Customer Responsibilities |
| **PE-3 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * physical access audit logs are maintained for entry or exit points; * access to areas within the facility designated as publicly accessible are maintained by implementing physical access controls; and * physical access devices are inventoried at least annually. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities. * **TEST:** Organizational processes for physical access control; mechanisms supporting and/or implementing physical access control; physical access control devices. |
| **PE-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-6 Monitoring Physical Access (Conditional)

|  |
| --- |
| **PE-6 Control Requirement(s)** |
| a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;  b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and  **PE-6 (b) Additional FedRAMP Requirements and Guidance:** [at least monthly]  c. Coordinate results of reviews and investigations with the organizational incident response capability. |
| **PE-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-6 What is the solution and how is it implemented?** |
| Description of how PE-6 is implemented,  Customer Responsibilities |
| **PE-6 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if physical access to the facility where the system resides is monitored to detect and respond to physical security incidents. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities. * **TEST:** Organizational processes for monitoring physical access; mechanisms supporting and/or implementing physical access monitoring; mechanisms supporting and/or implementing the review of physical access logs. |
| **PE-6 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-8 Visitor Access Records (Conditional)

|  |
| --- |
| **PE-8 Control Requirement(s)** |
| a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period];  **PE-8 (a) Additional FedRAMP Requirements and Guidance:** [for a minimum of one (1) year]  b. Review visitor access records [Assignment: organization-defined frequency]; and  **PE-8 (b) Additional FedRAMP Requirements and Guidance:** [at least monthly]  c. Report anomalies in visitor access records to [Assignment: organization-defined personnel]. |
| **PE-8 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-8 What is the solution and how is it implemented?** |
| Description of how PE-8 is implemented,  Customer Responsibilities |
| **PE-8 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * visitor access records for the facility where the system resides are maintained for a minimum of one (1) year; * visitor access records are reviewed at least monthly; and * visitor access records anomalies are reported to personnel. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing visitor access records; visitor access control logs or records; visitor access record or log reviews; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records. * **INTERVIEW:** Organizational personnel with visitor access record responsibilities; organizational personnel with information security and privacy responsibilities. * **TEST:** Organizational processes for maintaining and reviewing visitor access records; mechanisms supporting and/or implementing the maintenance and review of visitor access records. |
| **PE-8 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-8 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-12 Emergency Lighting (Conditional)

|  |
| --- |
| **PE-12 Control Requirement(s)** |
| Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. |
| **PE-12 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-12 What is the solution and how is it implemented?** |
| Description of how PE-12 is implemented,  Customer Responsibilities |
| **PE-12 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * automatic emergency lighting that activates in the event of a power outage or disruption is employed for the system; * automatic emergency lighting that activates in the event of a power outage or disruption is maintained for the system; * automatic emergency lighting for the system covers emergency exits within the facility; and * automatic emergency lighting for the system covers evacuation routes within the facility. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with the responsibility for emergency lighting and/or planning; organizational personnel with information security responsibilities. * **TEST:** Mechanisms supporting and/or implementing an emergency lighting capability. |
| **PE-12 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-12 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-13 Fire Protection (Conditional)

|  |
| --- |
| **PE-13 Control Requirement(s)** |
| Employ and maintain fire detection and suppression systems that are supported by an independent energy source. |
| **PE-13 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-13 What is the solution and how is it implemented?** |
| Description of how PE-13 is implemented,  Customer Responsibilities |
| **PE-13 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * fire detection systems are employed; * employed fire detection systems are supported by an independent energy source; * employed fire detection systems are maintained; * fire suppression systems are employed; * employed fire suppression systems are supported by an independent energy source; and * employed fire suppression systems are maintained. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with information security responsibilities. * **TEST:** Mechanisms supporting and/or implementing fire suppression/detection devices/systems. |
| **PE-13 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-13 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-14 Environmental Controls (Conditional)

|  |
| --- |
| **PE-14 Control Requirement(s)** |
| a. Maintain [Assignment: temperature; humidity; pressure; radiation] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and  **PE-14 (a) Additional FedRAMP Requirements and Guidance:** [consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments]  **PE-14 (a)** **Additional FedRAMP Requirements and Guidance:** The service provider measures temperature at server inlets and humidity levels by dew point.  b. Monitor environmental control levels [Assignment: organization-defined frequency].  **PE-14 (b) Additional FedRAMP Requirements and Guidance:** [continuously] |
| **PE-14 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-14 What is the solution and how is it implemented?** |
| Description of how PE-14 is implemented,  Customer Responsibilities |
| **PE-14 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments levels are maintained at acceptable levels within the facility where the system resides; and * environmental control levels are monitored continuously. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing temperature and humidity control; temperature and humidity controls; facility housing the system; temperature and humidity controls documentation; temperature and humidity records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities. * **TEST:** Mechanisms supporting and/or implementing the maintenance and monitoring of temperature and humidity levels. |
| **PE-14 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-14 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-15 Water Damage Protection (Conditional)

|  |
| --- |
| **PE-15 Control Requirement(s)** |
| Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. |
| **PE-15 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-15 What is the solution and how is it implemented?** |
| Description of how PE-15 is implemented,  Customer Responsibilities |
| **PE-15 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * the system is protected from damage resulting from water leakage by providing master shutoff or isolation valves; * the master shutoff or isolation valves are accessible; * the master shutoff or isolation valves are working properly; and * the master shutoff or isolation valves are known to key personnel. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing water damage protection; facility housing the system; master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities. * **TEST:** Master water-shutoff valves; organizational process for activating master water shutoff. |
| **PE-15 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-15 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PE-16 Delivery and Removal (Conditional)

|  |
| --- |
| **PE-16 Control Requirement(s)** |
| a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and  **PE-16 (a) Additional FedRAMP Requirements and Guidance:** [all information system components]  b. Maintain records of the system components. |
| **PE-16 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PE-16 What is the solution and how is it implemented?** |
| Description of how PE-16 is implemented,  Customer Responsibilities |
| **PE-16 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if records of the system components are maintained. |
| **Assessment Procedures:**   * **EXAMINE:** Physical and environmental protection policy; procedures addressing the delivery and removal of system components from the facility; facility housing the system; records of items entering and exiting the facility; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with responsibilities for controlling system components entering and exiting the facility; organizational personnel with information security responsibilities. * **TEST:** Organizational process for authorizing, monitoring, and controlling system-related items entering and exiting the facility; mechanisms supporting and/or implementing, authorizing, monitoring, and controlling system-related items entering and exiting the facility. |
| **PE-16 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PE-16 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Planning (PL)

PL-2 System Security and Privacy Plans

|  |
| --- |
| **PL-2 Control Requirement(s)** |
| a. Develop security and privacy plans for the system that:  1. Are consistent with the organization’s enterprise architecture;  2. Explicitly define the constituent system components;  3. Describe the operational context of the system in terms of mission and business processes;  4. Identify the individuals that fulfill system roles and responsibilities;  5. Identify the information types processed, stored, and transmitted by the system;  6. Provide the security categorization of the system, including supporting rationale;  7. Describe any specific threats to the system that are of concern to the organization;  8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;  9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;  10. Provide an overview of the security and privacy requirements for the system;  11. Identify any relevant control baselines or overlays, if applicable;  12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;  13. Include risk determinations for security and privacy architecture and design decisions;  14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and  15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.  b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];  c. Review the plans [Assignment: organization-defined frequency];  **PL-2 (c) Additional FedRAMP Requirements and Guidance:** [at least annually]  d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and  e. Protect the plans from unauthorized disclosure and modification. |
| **PL-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PL-2 What is the solution and how is it implemented?** |
| Description of how PL-2 is implemented,  Customer Responsibilities |
| **PL-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if plans are reviewed at least annually. |
| **Assessment Procedures:**   * **EXAMINE:** Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; procedures addressing security and privacy plan reviews and updates; enterprise architecture documentation; system security plan; privacy plan; records of system security and privacy plan reviews and updates; security and privacy architecture and design documentation; risk assessments; risk assessment results; control assessment documentation; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities. * **TEST:** Organizational processes for system security and privacy plan development, review, update, and approval; mechanisms supporting the system security and privacy plan. |
| **PL-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PL-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

PL-8 Security and Privacy Architectures

|  |
| --- |
| **PL-8 Control Requirement(s)** |
| a. Develop security and privacy architectures for the system that:  1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;  2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;  3. Describe how the architectures are integrated into and support the enterprise architecture; and  4. Describe any assumptions about, and dependencies on, external systems and services;  b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and  **PL-8 (b) Additional FedRAMP Requirements and Guidance:** [at least annually and when a significant change occurs]  **PL-8 (b) Additional FedRAMP Requirements and Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.  c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions. |
| **PL-8 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PL-8 What is the solution and how is it implemented?** |
| Description of how PL-8 is implemented,  Customer Responsibilities |
| **PL-8 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if changes in the enterprise architecture are reviewed and updated at least annually and when a significant change occurs to reflect changes in the enterprise architecture. |
| **Assessment Procedures:**   * **EXAMINE:** Security and privacy planning policy; procedures addressing information security and privacy architecture development; procedures addressing information security and privacy architecture reviews and updates; enterprise architecture documentation; information security and privacy architecture documentation; system security plan; privacy plan; security and privacy CONOPS for the system; records of information security and privacy architecture reviews and updates; other relevant documents or records. * **INTERVIEW:** Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities. * **TEST:** Organizational processes for developing, reviewing, and updating the information security and privacy architecture; mechanisms supporting and/or implementing the development, review, and update of the information security and privacy architecture. |
| **PL-8 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PL-8 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Personnel Security (PS)

PS-3 Personnel Screening

|  |
| --- |
| **PS-3 Control Requirement(s)** |
| a. Screen individuals prior to authorizing access to the system; and  b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].  **PS-3 (b) Additional FedRAMP Requirements and Guidance:** [for national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance.  For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low-risk positions] |
| **PS-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **PS-3 What is the solution and how is it implemented?** |
| Description of how PS-3 is implemented,  Customer Responsibilities |
| **PS-3 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if individuals are screened prior to authorizing access to the system. |
| **Assessment Procedures:**   * **EXAMINE:** Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities. * **TEST:** Organizational processes for personnel screening. |
| **PS-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **PS-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Risk Assessment (RA)

RA-2 Security Categorization

|  |
| --- |
| **RA-2 Control Requirement(s)** |
| a. Categorize the system and information it processes, stores, and transmits;  b. Document the security categorization results, including supporting rationale, in the security plan for the system; and  c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision. |
| **RA-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **RA-2 What is the solution and how is it implemented?** |
| Description of how RA-2 is implemented,  Customer Responsibilities |
| **RA-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * the system and the information it processes, stores, and transmits are categorized; * the security categorization results, including supporting rationale, are documented in the security plan for the system; and * the authorizing official or authorizing official designated representative reviews and approves the security categorization decision. |
| **Assessment Procedures:**   * **EXAMINE:** Risk assessment policy; security planning policy and procedures; procedures addressing security categorization of organizational information and systems; security categorization documentation; system security plan; privacy plan; other relevant documents or records. * **INTERVEIW:** Organizational personnel with security categorization and risk assessment responsibilities; organizational personnel with security and privacy responsibilities. * **TEST:** Organizational processes for security categorization. |
| **RA-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **RA-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

RA-3 Risk Assessment

|  |
| --- |
| **RA-3 Control Requirement(s)** |
| a. Conduct a risk assessment, including:  1. Identifying threats to and vulnerabilities in the system;  2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and  3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;  b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;  c. Document risk assessment results in [Assignment: security and privacy plans; risk assessment report];  **RA-3 (c) Additional FedRAMP Requirements and Guidance:** [security assessment report]  d. Review risk assessment results [Assignment: organization-defined frequency];  **RA-3 (d) Additional FedRAMP Requirements and Guidance:** [at least every three (3) years and when a significant change occurs]  e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and  **RA-3 (e) Additional FedRAMP Requirements and Guidance: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.**  f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.  **RA-3 (f) Additional FedRAMP Requirements and Guidance:** [at least every three (3) years]  **RA-3 Additional FedRAMP Requirements and Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F. |
| **RA-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **RA-3 What is the solution and how is it implemented?** |
| Description of how RA-3 is implemented,  Customer Responsibilities |
| **RA-3 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * risk assessment results and risk management decisions from the organization and mission or business process perspectives are integrated with system-level risk assessments; * risk assessment results are documented in security assessment report; * risk assessment results are reviewed at least every three (3) years and when a significant change occurs; * risk assessment results are disseminated to personnel or roles; and * the risk assessment is updated at least every three (3) years or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system. |
| **Assessment Procedures:**   * **EXAMINE:** Risk assessment policy; risk assessment procedures; security and privacy planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with risk assessment responsibilities; organizational personnel with security and privacy responsibilities. * **TEST:** Organizational processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the risk assessment. |
| **RA-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **RA-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

RA-5 Vulnerability Monitoring and Scanning

|  |
| --- |
| **RA-5 Control Requirement(s)** |
| a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;  **RA-5 (a) Additional FedRAMP Requirements and Guidance:** [monthly operating system/infrastructure; monthly web applications (including APIs) and databases].  **RA-5 (a) Additional FedRAMP Requirements and Guidance:** an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.  b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:  1. Enumerating platforms, software flaws, and improper configurations;  2. Formatting checklists and test procedures; and  3. Measuring vulnerability impact;  c. Analyze vulnerability scan reports and results from vulnerability monitoring;  d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;  **RA-5 (d) Additional FedRAMP Requirements and Guidance:** [high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery].  **RA-5 (d) Additional FedRAMP Requirements and Guidance:** If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog (<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>) the KEV remediation date supersedes the FedRAMP parameter requirement.  e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and  **RA-5 (e) Additional FedRAMP Requirements and Guidance:** to include all Authorizing Officials; for JAB authorizations to include FedRAMP.  f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.  **RA-5 Additional FedRAMP Requirements and Guidance:** **See the FedRAMP Documents page> Vulnerability Scanning Requirements** [**https://www.FedRAMP.gov/documents/**](https://www.fedramp.gov/documents/)  **RA-5 Additional FedRAMP Requirements and Guidance:** Informational findings from a scanner are detailed as a returned result that holds no vulnerability risk or severity and for FedRAMP does not require an entry onto the POA&M or entry onto the RET during any assessment phase.  Warning findings, on the other hand, are given a risk rating (low, moderate, high or critical) by the scanning solution and should be treated like any other finding with a risk or severity rating for tracking purposes onto either the POA&M or RET depending on when the findings originated (during assessments or during monthly continuous monitoring). If a warning is received during scanning, but further validation turns up no actual issue then this item should be categorized as a false positive. If this situation presents itself during an assessment phase (initial assessment, annual assessment or any SCR), follow guidance on how to report false positives in the Security Assessment Report (SAR). If this situation happens during monthly continuous monitoring, a deviation request will need to be submitted per the FedRAMP Vulnerability Deviation Request Form.  Warnings are commonly associated with scanning solutions that also perform compliance scans, and if the scanner reports a “warning” as part of the compliance scanning of a CSO, follow guidance surrounding the tracking of compliance findings during either the assessment phases (initial assessment, annual assessment or any SCR) or monthly continuous monitoring as it applies. Guidance on compliance scan findings can be found by searching on “Tracking of Compliance Scans” in FAQs. |
| **RA-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **RA-5 What is the solution and how is it implemented?** |
| Description of how RA-5 is implemented,  Customer Responsibilities |
| **RA-5 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * vulnerability monitoring tools and techniques are employed to facilitate interoperability among tools; * vulnerability scan reports and results from vulnerability monitoring are analyzed; * legitimate vulnerabilities are remediated high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery in accordance with an organizational assessment of risk; * information obtained from the vulnerability monitoring process and control assessments is shared with Personnel or roles to help eliminate similar vulnerabilities in other systems; and * vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned are employed. |
| **Assessment Procedures:**   * **EXAMINE:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with vulnerability remediation responsibilities; organizational personnel with security responsibilities; system/network administrators. * **TEST:** Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing. |
| **RA-5 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **RA-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

RA-5(2) Update Vulnerabilities to Be Scanned

|  |
| --- |
| **RA-5(2) Control Requirement(s)** |
| Update the system vulnerabilities to be scanned [Assignment: prior to a new scan; when new vulnerabilities are identified and reported].  **RA-5 (2) Additional FedRAMP Requirements and Guidance:** [prior to a new scan] |
| **RA-5(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **RA-5(2) What is the solution and how is it implemented?** |
| Description of how RA-5(2) is implemented,  Customer Responsibilities |
| **RA-5(2) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if the system vulnerabilities to be scanned are updated prior to a new scan. |
| **Assessment Procedures:**   * **EXAMINE:** Procedures addressing vulnerability scanning; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities; system/network administrators. * **TEST:** Organizational processes for vulnerability scanning; mechanisms/tools supporting and/or implementing vulnerability scanning. |
| **RA-5(2) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **RA-5(2) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

RA-5(11) Public Disclosure Program

|  |
| --- |
| **RA-5(11) Control Requirement(s)** |
| Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components. |
| **RA-5(11) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **RA-5(11) What is the solution and how is it implemented?** |
| Description of how RA-5(11) is implemented,  Customer Responsibilities |
| **RA-5(11) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if a public reporting channel is established for receiving reports of vulnerabilities in organizational systems and system components. |
| **Assessment Procedures:**   * **EXAMINE:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; vulnerability management records; audit records; public reporting channel; system security plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities. * **TEST:** Organizational processes for vulnerability scanning; mechanisms/tools supporting and/or implementing vulnerability scanning; mechanisms implementing the public reporting of vulnerabilities. |
| **RA-5(11) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **RA-5(11) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

RA-7 Risk Response

|  |
| --- |
| **RA-7 Control Requirement(s)** |
| Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance. |
| **RA-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **RA-7 What is the solution and how is it implemented?** |
| Description of how RA-7 is implemented,  Customer Responsibilities |
| **RA-7 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * findings from security assessments are responded to in accordance with organizational risk tolerance; * findings from privacy assessments are responded to in accordance with organizational risk tolerance; * findings from monitoring are responded to in accordance with organizational risk tolerance; and * findings from audits are responded to in accordance with organizational risk tolerance. |
| **Assessment Procedures:**   * **EXAMINE:** Risk assessment policy; assessment reports; audit records/event logs; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with assessment and auditing responsibilities; system/network administrators; organizational personnel with security and privacy responsibilities. * **TEST:** Organizational processes for assessments and audits; mechanisms/tools supporting and/or implementing assessments and auditing. |
| **RA-7 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **RA-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## System and Services Acquisition (SA)

SA-9 External System Services

|  |
| --- |
| **SA-9 Control Requirement(s)** |
| a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];  **SA-9 (a) Additional FedRAMP Requirements and Guidance:** [Appropriate FedRAMP Security Controls Baseline (s) if Federal information is processed or stored within the external system]  b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and  c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].  **SA-9 (c) Additional FedRAMP Requirements and Guidance:** [Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored] |
| **SA-9 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SA-9 What is the solution and how is it implemented?** |
| Description of how SA-9 is implemented,  Customer Responsibilities |
| **SA-9 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored are employed to monitor control compliance by external service providers on an ongoing basis. |
| **Assessment Procedures:**   * **EXAMINE:** System and services acquisition policy; system and services acquisition procedures; procedures addressing methods and techniques for monitoring control compliance by external service providers of system services; acquisition documentation; contracts; service level agreements; interagency agreements; licensing agreements; list of organizational security and privacy requirements for external provider services; control assessment results or reports from external providers of system services; system security plan; privacy plan; supply chain risk management plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with acquisition responsibilities; external providers of system services; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities. * **TEST:** Organizational processes for monitoring security and privacy control compliance by external service providers on an ongoing basis; mechanisms for monitoring security and privacy control compliance by external service providers on an ongoing basis. |
| **SA-9 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SA-9 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SA-22 Unsupported System Components

|  |
| --- |
| **SA-22 Control Requirement(s)** |
| a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or  b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]]. |
| **SA-22 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SA-22 What is the solution and how is it implemented?** |
| Description of how SA-22 is implemented,  Customer Responsibilities |
| **SA-22 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer; and * in-house support; support from external providers provide options for alternative sources for continued support for unsupported components. |
| **Assessment Procedures:**   * **EXAMINE:** System and services acquisition policy; procedures addressing the replacement or continued use of unsupported system components; documented evidence of replacing unsupported system components; documented approvals (including justification) for the continued use of unsupported system components; system security plan; supply chain risk management plan; other relevant documents or records. * **INTERVIEW:** Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with the responsibility for the system development life cycle; organizational personnel responsible for component replacement. * **TEST:** Organizational processes for replacing unsupported system components; mechanisms supporting and/or implementing the replacement of unsupported system components. |
| **SA-22 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SA-22 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## System and Communications Protection (SC)

SC-5 Denial of Service Protection (Conditional)

|  |
| --- |
| **SC-5 Control Requirement(s)** |
| a. [Assignment: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: Protect against; Limit]; and [Assignment: organization-defined types of denial-of-service events]  **SC-5 (a)-1 Additional FedRAMP Requirements and Guidance:** [Protect against]  **SC-5 (a)-2 Additional FedRAMP Requirements and Guidance:** [at a minimum: ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack]  b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event]. |
| **SC-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-5 What is the solution and how is it implemented?** |
| Description of how SC-5 is implemented,  Customer Responsibilities |
| **SC-5 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * the effects of at a minimum: ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack are protected against; and * controls by type of denial-of-service event are employed to achieve the denial-of-service protection objective. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; list of denial-of-service attacks requiring employment of security safeguards to protect against or limit effects of such attacks; list of security safeguards protecting against or limiting the effects of denial-of-service attacks; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer. * **TEST:** Mechanisms protecting against or limiting the effects of denial-of-service attacks. |
| **SC-5 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SC-7 Boundary Protection

|  |
| --- |
| **SC-7 Control Requirement(s)** |
| a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;  b. Implement subnetworks for publicly accessible system components that are [Assignment: physically; logically] separated from internal organizational networks; and  **SC-7 (b) Additional FedRAMP Requirements and Guidance:** SC-7 (b) should be met by subnet isolation. A subnetwork (subnet) is a physically or logically segmented section of a larger network defined at TCP/IP Layer 3, to both minimize traffic and, important for a FedRAMP Authorization, add a crucial layer of network isolation. Subnets are distinct from VLANs (Layer 2), security groups, and VPCs and are specifically required to satisfy SC-7 part b and other controls. See the FedRAMP Subnets White Paper (<https://www.fedramp.gov/assets/resources/documents/FedRAMP_subnets_white_paper.pdf>) for additional information.  c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture. |
| **SC-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-7 What is the solution and how is it implemented?** |
| Description of how SC-7 is implemented,  Customer Responsibilities |
| **SC-7 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * subnetworks for publicly accessible system components are physically; logically separated from internal organizational networks; and * external networks or systems are only connected to through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. * **TEST:** Mechanisms implementing boundary protection capabilities. |
| **SC-7 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SC-8 Transmission Confidentiality and Integrity

|  |
| --- |
| **SC-8 Control Requirement(s)** |
| Protect the [Assignment: confidentiality; integrity] of transmitted information.  **SC-8 Additional FedRAMP Requirements and Guidance:** For each instance of data in transit, confidentiality AND integrity should be through cryptography as specified in SC-8 (1), physical means as specified in SC-8 (5), or in combination.  For clarity, this control applies to all data in transit. Examples include the following data flows:  - Crossing the system boundary  - Between compute instances - including containers  - From a compute instance to storage  - Replication between availability zones  - Transmission of backups to storage  - From a load balancer to a compute instance  - Flows from management tools required for their work – e.g. log collection, scanning, etc.  The following applies only when choosing SC-8 (5) in lieu of SC-8 (1).  FedRAMP-Defined Assignment / Selection Parameters  SC-8 (5)-1 [a hardened or alarmed carrier Protective Distribution System (PDS) when outside of Controlled Access Area (CAA)]  SC-8 (5)-2 [prevent unauthorized disclosure of information AND detect changes to information]  SC-8 (5) applies when physical protection has been selected as the method to protect confidentiality and integrity. For physical protection, data in transit must be in either a Controlled Access Area (CAA), or a Hardened or alarmed PDS.  Hardened or alarmed PDS: Shall be as defined in SECTION X - CATEGORY 2 PDS INSTALLATION GUIDANCE of CNSSI No.7003, titled PROTECTED DISTRIBUTION SYSTEMS (PDS). Per the CNSSI No. 7003 Section VIII, PDS must originate and terminate in a Controlled Access Area (CAA).  Controlled Access Area (CAA): Data will be considered physically protected, and in a CAA if it meets Section 2.3 of the DHS’s Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. CSPs can meet Section 2.3 of the DHS’ recommended practice by satisfactory implementation of the following controls PE-2 (1), PE-2 (2), PE-2 (3), PE-3 (2), PE-3 (3), PE-6 (2), and PE-6 (3).  Note: When selecting SC-8 (5), the above SC-8(5), and the above referenced PE controls must be added to the SSP.  CNSSI No.7003 can be accessed here:  <https://www.dcsa.mil/Portals/91/documents/ctp/nao/CNSSI_7003_PDS_September_2015.pdf>  DHS Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies can be accessed here: <https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf> |
| **SC-8 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-8 What is the solution and how is it implemented?** |
| Description of how SC-8 is implemented,  Customer Responsibilities |
| **SC-8 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if the confidentiality; integrity of transmitted information is/are protected. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; system developer. * **TEST:** Mechanisms supporting and/or implementing transmission confidentiality and/or integrity. |
| **SC-8 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-8 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SC-8(1) Cryptographic Protection

|  |
| --- |
| **SC-8(1) Control Requirement(s)** |
| Implement cryptographic mechanisms to [Assignment: prevent unauthorized disclosure of information; detect changes to information] during transmission.  **SC-8 (1) Additional FedRAMP Requirements and Guidance:** Please ensure SSP Section 10.3 Cryptographic Modules Implemented for Data at Rest (DAR) and Data In Transit (DIT) is fully populated for reference in this control.  **SC-8 (1) Additional FedRAMP Requirements and Guidance:** See M-22-09, including "Agencies encrypt all DNS requests and HTTP traffic within their environment."  **SC-8 (1)** applies when encryption has been selected as the method to protect confidentiality and integrity. Otherwise refer to SC-8 (5). SC-8 (1) is strongly encouraged.  **SC-8 (1) Additional FedRAMP Requirements and Guidance:** Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)  **SC-8 (1)** **Additional FedRAMP Requirements and Guidance:** When leveraging encryption from the underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured. |
| **SC-8(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-8(1) What is the solution and how is it implemented?** |
| Description of how SC-8(1) is implemented,  Customer Responsibilities |
| **SC-8(1) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if cryptographic mechanisms are implemented to prevent unauthorized disclosure of information; detect changes to information during transmission. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; system developer. * **TEST:** Cryptographic mechanisms supporting and/or implementing transmission confidentiality and/or integrity; mechanisms supporting and/or implementing alternative physical safeguards; organizational processes for defining and implementing alternative physical safeguards. |
| **SC-8(1) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-8(1) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SC-12 Cryptographic Key Establishment and Management

|  |
| --- |
| **SC-12 Control Requirement(s)** |
| Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].  **SC-12 Additional FedRAMP Requirements and Guidance:** [In accordance with Federal requirements]  **SC-12 Additional FedRAMP Requirements and Guidance:** See references in NIST 800-53 documentation.  **SC-12 Additional FedRAMP Requirements and Guidance:** Must meet applicable Federal Cryptographic Requirements. See References Section of control.  **SC-12** **Additional FedRAMP Requirements and Guidance:** Wildcard certificates may be used internally within the system but are not permitted for external customer access to the system. |
| **SC-12 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-12 What is the solution and how is it implemented?** |
| Description of how SC-12 is implemented,  Customer Responsibilities |
| **SC-12 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * cryptographic keys are established when cryptography is employed within the system in accordance with Federal requirements; and * cryptographic keys are managed when cryptography is employed within the system in accordance with Federal requirements. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; cryptographic mechanisms; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for cryptographic key establishment and/or management. * **TEST:** Mechanisms supporting and/or implementing cryptographic key establishment and management. |
| **SC-12 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-12 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SC-13 Cryptographic Protection (Conditional)

|  |
| --- |
| **SC-13 Control Requirement(s)** |
| a. Determine the [Assignment: organization-defined cryptographic uses]; and  b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].  **SC-13 (b) Additional FedRAMP Requirements and Guidance:** [FIPS-validated or NSA-approved cryptography]  **SC-13** **Additional FedRAMP Requirements and Guidance:**  This control applies to all use of cryptography. In addition to encryption, this includes functions such as hashing, random number generation, and key generation. Examples include the following:  - Encryption of data  - Decryption of data  - Generation of one-time passwords (OTPs) for MFA  - Protocols such as TLS, SSH, and HTTPS  The requirement for FIPS 140 validation, as well as timelines for acceptance of FIPS 140-2, and 140-3 can be found at the NIST Cryptographic Module Validation Program (CMVP).  <https://csrc.nist.gov/projects/cryptographic-module-validation-program>  **SC-13** **Additional FedRAMP Requirements and Guidance:** For NSA-approved cryptography, the National Information Assurance Partnership (NIAP) oversees a national program to evaluate Commercial IT Products for Use in National Security Systems. The NIAP Product Compliant List can be found at the following location: <https://www.niap-ccevs.org/Product/index.cfm>  **SC-13** **Additional FedRAMP Requirements and Guidance:** When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.  **SC-13** **Additional FedRAMP Requirements and Guidance:**  Moving to non-FIPS CM or product is acceptable when:  - FIPS validated version has a known vulnerability  - Feature with vulnerability is in use  - Non-FIPS version fixes the vulnerability  - Non-FIPS version is submitted to NIST for FIPS validation  - POA&M is added to track approval, and deployment when ready  **SC-13** **Additional FedRAMP Requirements and Guidance:** At a minimum, this control applies to cryptography in use for the following controls: AU-9(3), CP-9(8), IA-2(6), IA-5(1), MP-5, SC-8(1), and SC-28(1). |
| **SC-13 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-13 What is the solution and how is it implemented?** |
| Description of how SC-13 is implemented,  Customer Responsibilities |
| **SC-13 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * cryptographic uses are identified; and * FIPS-validated or NSA-approved cryptography for each specified cryptographic use (defined in SC-13\_ODP[01]) are implemented. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing cryptographic protection; system design documentation; system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic protection. * **TEST:** Mechanisms supporting and/or implementing cryptographic protection. |
| **SC-13 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-13 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SC-28 Protection of Information at Rest

|  |
| --- |
| **SC-28 Control Requirement(s)** |
| Protect the [Assignment: confidentiality/integrity] of the following information at rest: [Assignment: organization-defined information at rest].  **SC-28** **Additional FedRAMP Requirements and Guidance:** The organization supports the capability to use cryptographic mechanisms to protect information at rest.  **SC-28** **Additional FedRAMP Requirements and Guidance:** When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.  **SC-28** **Additional FedRAMP Requirements and Guidance:** Note that this enhancement requires the use of cryptography in accordance with SC-13. |
| **SC-28 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-28 What is the solution and how is it implemented?** |
| Description of how SC-28 is implemented,  Customer Responsibilities |
| **SC-28 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if the confidentiality; integrity of information at rest is/are protected. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; system developer. * **TEST:** Mechanisms supporting and/or implementing confidentiality and integrity protections for information at rest. |
| **SC-28 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-28 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SC-28(1) Cryptographic Protection

|  |
| --- |
| **SC-28(1) Control Requirement(s)** |
| Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].  **SC-28 (1)-1 Additional FedRAMP Requirements and Guidance:** [all information system components storing Federal data or system data that must be protected at the High or Moderate impact levels]  **SC-28 (1)** **Additional FedRAMP Requirements and Guidance:**  Organizations should select a mode of protection that is targeted towards the relevant threat scenarios.  Examples:  A. Organizations may apply full disk encryption (FDE) to a mobile device where the primary threat is loss of the device while storage is locked.  B. For a database application housing data for a single customer, encryption at the file system level would often provide more protection than FDE against the more likely threat of an intruder on the operating system accessing the storage.  C. For a database application housing data for multiple customers, encryption with unique keys for each customer at the database record level may be more appropriate. |
| **SC-28(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SC-28(1) What is the solution and how is it implemented?** |
| Description of how SC-28(1) is implemented,  Customer Responsibilities |
| **SC-28(1) Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * cryptographic mechanisms are implemented to prevent unauthorized disclosure of information at rest on all information system components storing Federal data or system data that must be protected at the High or Moderate impact levels; and * cryptographic mechanisms are implemented to prevent unauthorized modification of information at rest on all information system components storing Federal data or system data that must be protected at the High or Moderate impact levels. |
| **Assessment Procedures:**   * **EXAMINE:** System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; system developer. * **TEST:** Cryptographic mechanisms implementing confidentiality and integrity protections for information at rest. |
| **SC-28(1) Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SC-28(1) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## System and Information Integrity (SI)

SI-2 Flaw Remediation

|  |
| --- |
| **SI-2 Control Requirement(s)** |
| a. Identify, report, and correct system flaws;  b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;  c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and  **SI-2 (c) Additional FedRAMP Requirements and Guidance:** [within thirty (30) days of release of updates]  d. Incorporate flaw remediation into the organizational configuration management process. |
| **SI-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SI-2 What is the solution and how is it implemented?** |
| Description of how SI-2 is implemented,  Customer Responsibilities |
| **SI-2 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if flaw remediation is incorporated into the organizational configuration management process. |
| **Assessment Procedures:**   * **EXAMINE:** System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; procedures addressing configuration management; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws)test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; system security plan; privacy plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel responsible for installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation; organizational personnel with configuration management responsibilities. * **TEST:** Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting and/or implementing the reporting and correcting of system flaws; mechanisms supporting and/or implementing testing software and firmware updates. |
| **SI-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SI-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SI-3 Malicious Code Protection

|  |
| --- |
| **SI-3 Control Requirement(s)** |
| a. Implement [Assignment: signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;  **SI-3 (a) Additional FedRAMP Requirements and Guidance:** [signature based and non-signature based]  b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;  c. Configure malicious code protection mechanisms to:  1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Assignment: organization-defined frequency] as the files are downloaded, opened, or executed in accordance with organizational policy; and [Assignment: endpoint; network entry and exit points]  **SI-3 (c) (1)-1 Additional FedRAMP Requirements and Guidance:** [at least weekly]  **SI-3 (c) (1)-2 Additional FedRAMP Requirements and Guidance:** [to include endpoints and network entry and exit points]  2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and  **SI-3 (c) (2)-1 Additional FedRAMP Requirements and Guidance:** [to include blocking and quarantining malicious code]  **SI-3 (c) (2)-2 Additional FedRAMP Requirements and Guidance:** [administrator or defined security personnel near-real time]  d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system. |
| **SI-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SI-3 What is the solution and how is it implemented?** |
| Description of how SI-3 is implemented,  Customer Responsibilities |
| **SI-3 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * malicious code protection mechanisms are updated automatically as new releases are available in accordance with organizational configuration management policy and procedures; and * the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system are addressed. |
| **Assessment Procedures:**   * **EXAMINE:** System and information integrity policy; system and information integrity procedures; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit records; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for malicious code protection; organizational personnel with configuration management responsibilities. * **TEST:** Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational processes for addressing false positives and resulting potential impacts; mechanisms supporting and/or implementing, employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting and/or implementing malicious code scanning and subsequent actions. |
| **SI-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SI-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

SI-4 System Monitoring

|  |
| --- |
| **SI-4 Control Requirement(s)** |
| a. Monitor the system to detect:  1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and  2. Unauthorized local, network, and remote connections;  b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];  c. Invoke internal monitoring capabilities or deploy monitoring devices:  1. Strategically within the system to collect organization-determined essential information; and  2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;  d. Analyze detected events and anomalies;  e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;  f. Obtain legal opinion regarding system monitoring activities; and  g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles].  **SI-4 Additional FedRAMP Requirements and Guidance:** See US-CERT Incident Response Reporting Guidelines. |
| **SI-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from Pre-Existing Authorization for <CSP Name here>, Date of Authorization |
| **SI-4 What is the solution and how is it implemented?** |
| Description of how SI-4 is implemented,  Customer Responsibilities |
| **SI-4 Assessment Plan/Procedures** |
| **Assessment Objective:**  Determine if:   * unauthorized use of the system is identified through techniques and methods; * the level of system monitoring activity is adjusted when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; * a legal opinion regarding system monitoring activities is obtained; and * system monitoring information is provided to personnel or roles. |
| **Assessment Procedures:**   * **EXAMINE:** System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; facility diagram/layout; system design documentation; system monitoring tools and techniques documentation; locations within the system where monitoring devices are deployed; system configuration settings and associated documentation; system security plan; other relevant documents or records. * **INTERVIEW:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system. * **TEST:** Organizational processes for system monitoring; mechanisms supporting and/or implementing system monitoring capabilities. |
| **SI-4 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system |
| **SI-4 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

# 2.0 FedRAMP LI-SaaS Assessment Results

The assessment was performed by <assessor> and took place between <*date*> and <*date*>. The assessment was conducted in accordance with the assessment plans/procedures defined in this FedRAMP *Tailored* LI-SaaS Framework. All assessment activities documented to occur as described in the assessment plan <*did / did not*> take place as described. <*describe exceptions as applicable*>.

Table A-4, Summary of Assessment Results, represents the aggregate risk identified from the FedRAMP assessment. This table should include all risks, including the risks identified in *all vulnerability scans.*

Table A-4. Summary of Assessment Results

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Total** | **Operational Requirement** | **Vendor Dependency** |
| High | [Number] | N/A | N/A |
| High risk adjusted to Moderate | [Number] | [Number] | [Number] |
| Moderate | [Number] | [Number] | [Number] |
| High risk adjusted to Low | [Number] | [Number] | [Number] |
| Moderate risk adjusted to Low | [Number] | [Number] | [Number] |
| Low | [Number] | [Number] | [Number] |
| **Total Risks** | **[Number]** | [Number] | [Number] |

<Instruction: Note: All highs must be remediated prior to the assessor recommending the CSO for FedRAMP Authorization. Some High vulnerabilities may be downgraded to moderate due to mitigating factors. If the assessor believes there is justification that a High finding can be downgraded to a Moderate finding, the assessor must submit a strong Deviation Rationale along with the Risk Adjustment in the Risk Exposure Table. The JAB ***does not typically allow*** any high vulnerabilities risk adjusted to low. Nor does the JAB accept High vulnerabilities as Operational Requirements.>

The assessment took place from <m/d/yyyy to m/d/yyyy and m/d/yyyy to m/d/yyyy>. Below is a summary of the vulnerabilities found during this assessment. Please refer to the Risk Exposure Table Workbook for additional details.

*The RET is the same RET template that is used for the Security Assessment Report (SAR) for all other baselines.*

The RET is embedded here. <name of file>

The 3PAO completed LI-SaaS Penetration Test Report is embedded here. <name of file>

# 3.0 FedRAMP LI-SaaS [System Name] Attestation Statement

The system owner’s signature for this SSP serves as the attestation for the following sections.

## Attestation of Policies and Procedures

The following policies and procedures exist and address the basic elements listed for this system. The policies are reviewed and updated at least every three years. The procedures are reviewed and updated annually. Exceptions are identified in the *Modifications* column.

Where policies or procedures are fully inherited, simply state, “This is inherited.” in the Modification Statement column. For a fully virtual SaaS this is likely true for PE-1, Physical and Environment Protection Policy and Procedures, and may be true for others.

**Do not delete rows or modify the Basic Elements column in the tables below. State any exceptions in the Modifications Statement column.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Control ID** | **Control Name** | **Basic Elements** | **Modification Statement** |
| 1. | AC-1 | Policy and Procedures | * An access control policy is developed, documented and disseminated to CSP-defined personnel or roles. * Access control procedures to facilitate the implementation of the access control policy and associated access controls are developed, documented and disseminated to CSP-defined personnel or roles. * The access control policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The access control policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the access control policy and procedures. * The current access control policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current access control procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 2. | AT-1 | Policy and Procedures | * An awareness and training policy is developed, documented and disseminated to CSP-defined personnel or roles. * Awareness and training procedures to facilitate the implementation of the awareness and training policy and associated awareness and training controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The awareness and training policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The awareness and training policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the awareness and training policy and procedures. * The current awareness and training policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current awareness and training procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 3. | AU-1 | Policy and Procedures | * An audit and accountability policy is developed, documented and disseminated to CSP-defined personnel or roles. * Audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The audit and accountability policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The audit and accountability policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the audit and accountability policy and procedures. * The current audit and accountability policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current audit and accountability procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 4. | CA-1 | Policy and Procedures | * An assessment, authorization, and monitoring policy is developed, documented and disseminated to CSP-defined personnel or roles. * Assessment, authorization, and monitoring procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and associated assessment, authorization, and monitoring controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The assessment, authorization, and monitoring policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The assessment, authorization, and monitoring policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures. * The current assessment, authorization, and monitoring policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current assessment, authorization, and monitoring procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 5. | CM-1 | Policy and Procedures | * A configuration management policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Configuration management procedures to facilitate the implementation of the configuration management policy and associated configuration management controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The configuration management policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The configuration management policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the configuration management policy and procedures. * The current configuration management policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current configuration management procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 6. | CP-1 | Policy and Procedures | * A contingency planning policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Contingency planning procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The contingency planning policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The contingency planning policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the contingency planning policy and procedures. * The current contingency planning policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current contingency planning procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 7. | IA-1 | Policy and Procedures | * An identification and authentication policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Identification and authentication procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The identification and authentication policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The identification and authentication policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the identification and authentication policy and procedures. * The current identification and authentication policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current identification and authentication procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 8. | IR-1 | Policy and Procedures | * An incident response policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Incident response procedures to facilitate the implementation of the incident response policy and associated incident response controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The incident response policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The incident response policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the incident response policy and procedures. * The current incident response policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current incident response procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 9. | MA-1 | Policy and Procedures | * A maintenance policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Maintenance procedures to facilitate the implementation of the maintenance policy and associated maintenance controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The maintenance policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The maintenance policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the maintenance policy and procedures. * The current maintenance policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current maintenance procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 10. | MP-1 | Policy and Procedures | * A media protection policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Media protection procedures to facilitate the implementation of the media protection policy and associated media protection controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The media protection policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The media protection policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the media protection policy and procedures. * The current media protection policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current media protection procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 11. | PE-1 | Policy and Procedures | * A physical and environmental protection policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Physical and environmental protection procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The physical and environmental protection policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The physical and environmental protection policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures. * The current physical and environmental protection policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current physical and environmental protection procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 12. | PL-1 | Policy and Procedures | * A planning policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Planning procedures to facilitate the implementation of the planning policy and associated planning controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The planning policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The planning policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the planning policy and procedures. * The current planning policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current planning procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 13. | PS-1 | Policy and Procedures | * A personnel security policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Personnel security procedures to facilitate the implementation of the personnel security policy and associated personnel security controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The personnel security policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The personnel security policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the personnel security policy and procedures. * The current personnel security policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current personnel security procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 14. | RA-1 | Policy and Procedures | * A risk assessment policy is developed, documented, and disseminated to CSP-defined personnel or roles. * Risk assessment procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The risk assessment policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The risk assessment policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the risk assessment policy and procedures. * The current risk assessment policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current risk assessment procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 15. | SA-1 | Policy and Procedures | * A system and services acquisition policy is developed, documented, and disseminated to CSP-defined personnel or roles. * System and services acquisition procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The system and services acquisition policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The system and services acquisition policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures. * The current system and services acquisition policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current system and services acquisition procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 16. | SC-1 | Policy and Procedures | * A system and communications protection policy is developed, documented, and disseminated to CSP-defined personnel or roles. * System and communications protection procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The system and communications protection policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The system and communications protection policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the system and communications protection policy and procedures. * The current system and communications protection policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current system and communications protection procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 17. | SI-1 | Policy and Procedures | * A system and information integrity policy is developed, documented, and disseminated to CSP-defined personnel or roles. * System and information integrity procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls are developed, documented, and disseminated to CSP-defined personnel or roles. * The system and information integrity policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The system and information integrity policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the system and information integrity policy and procedures. * The current system and information integrity policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current system and information integrity procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |
| 18. | SR-1 | Policy and Procedures | * A supply chain risk management policy is developed, documented, and disseminated to CSP-defined personnel or roles, to include Chief Privacy and ISSO and/or similar role or designees. * Supply chain risk management procedures to facilitate the implementation of the supply chain risk management policy and associated supply chain risk management controls are developed, documented, and disseminated to CSP-defined personnel or roles, to include chief privacy and ISSO and/or similar role or designees. * The supply chain risk management policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. * The supply chain risk management policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. * The CSP-defined official is designated to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures. * The current supply chain risk management policy is reviewed and updated at least every three (3) years and after organization-defined events. * The current supply chain risk management procedures are reviewed and updated at least annually; significant changes and after organization-defined events. |  |

## Attestation of Capabilities

The following capabilities exist and satisfy the associated requirement at least to the degree described in the associated attestation statement.

**Do not delete rows or modify the Attestation Statement column in the table below. State any exceptions in the Modifications column.**

Where the satisfaction of a control is partially or fully inherited, please check the appropriate box in the Modification Statement column. If there is no inheritance, leave both boxes unchecked. For example, if the PE controls are fully inherited from an underlying service provider with a separate authorization, check the “Inherited” box for each.

Please note, you are still attesting the statements for inherited controls are true to the best of your knowledge. If you have reason to believe otherwise, you must still state the difference in the Modification Statement column.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Control ID** | **Control Name** | **Attestation Statement** | **Modification Statement** |
| 1. | AC-20 | Use of External Systems | * CSP values are consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:   - access the system from external systems (if applicable); and  - process, store, or transmit organization-controlled information using external systems (if applicable).   * The use of CSP-defined prohibited types of external systems is prohibited (if applicable).   Additional FedRAMP Requirements/Guidance: Requirement: The interrelated controls of AC-20, CA-3, and SA-9 are differentiated as follows:   * AC-20 describes system access to and from external systems. * CA-3 describes documentation of an agreement between the respective system owners when data is exchanged between the CSO and an external system. * SA-9 describes the responsibilities of external system owners. These responsibilities would typically be captured in the agreement required by CA-3. | Inherited  Partially Inherited |
| 2. | AT-2 | Literacy Training and Awareness | * Security literacy training is provided to system users (including managers, senior executives, and contractors) as part of initial training for new users and at least annually thereafter. * Privacy literacy training is provided to system users (including managers, senior executives, and contractors) as part of initial training for new users and at least annually thereafter. * Security and privacy literacy training is provided to system users (including managers, senior executives, and contractors) when required by system changes or following significant changes. * CSP-defined awareness techniques are employed to increase the security and privacy awareness of system users. * Literacy training and awareness content is updated at least annually and after significant changes and after organization-defined events. * Lessons learned from internal or external security incidents or breaches are incorporated into literacy training and awareness techniques. | Inherited  Partially Inherited |
| 3. | AT-2(2) | Literacy Training and Awareness | * Literacy training on recognizing and reporting potential indicators of insider threat is provided. | Inherited  Partially Inherited |
| 4 | AT-3 | Role-based Training | * Role-based security and privacy training is provided to CSP-defined roles and responsibilities; at least annually and before authorizing access to the system, information, or performing assigned duties and organization-defined frequency thereafter. * Role-based training content is updated at least annually and after organization-defined events when required by system changes. * Lessons learned from internal or external security incidents or breaches are incorporated into role-based training. | Inherited  Partially Inherited |
| 5 | AT-4 | Training Records | * Information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training, are documented and monitored. * Individual training records are retained for at least one (1) year or 1 year after completion of specific training program. | Inherited  Partially Inherited |
| 6 | AU-2 | Event Logging | * 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 that the system is capable of logging are identified in support of the audit logging function. * The event logging function is coordinated with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged. * CSP-defined subset of the auditable events defined above to be audited continually for each identified event are specified for logging within the system. * The specified event types are logged within the system continuously. * A rationale is provided for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents. * Coordination between service provider and consumer is documented and accepted by the AO. * The event types selected for logging are reviewed and updated annually and whenever there is a change in the threat environment. | Inherited  Partially Inherited |
| 7 | AU-8 | Time Stamps | * Internal system clocks are used to generate timestamps for audit records. * Timestamps are recorded for audit records that meet one second of granularity of time measurement and that use coordinated universal time, have a fixed local time offset from coordinated universal time, or include the local time offset as part of the timestamp. | Inherited  Partially Inherited |
| 8 | AU-9 | Protection of Audit Information | * Audit information and audit logging tools are protected from unauthorized access, modification, and deletion. * CSP-defined personnel or roles are alerted upon detection of unauthorized access, modification, or deletion of audit information. | Inherited  Partially Inherited |
| 9 | AU-12 | Audit Record Generation | * Audit record generation capability for the event types the system is capable of auditing (events defined in AU-02) is provided by all information system and network components where audit capability is deployed/available. * CSP-defined personnel or roles is/are allowed to select the event types that are to be logged by specific components of the system. * Audit records for the event types defined in AU-02 that include the audit record content defined in AU-03 are generated. | Inherited  Partially Inherited |
| 10. | CA-2 (1) | Control Assessments | * Independent assessors or assessment teams are employed to conduct control assessments. | Inherited  Partially Inherited |
| 11 | CA-5 | Plan of Action and Milestones | * A Plan of Action and Milestones (POA&M) for the system is developed to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system. * Existing Plan of Action and Milestones are updated at least monthly based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities. | Inherited  Partially Inherited |
| 12 | CM-2 | Baseline Configuration | * A current baseline configuration of the system is developed, documented, and maintained under configuration control. * The baseline configuration of the system is reviewed and updated at least annually and when a significant change occurs. * The baseline configuration of the system is reviewed and updated when required by the JAB/AO. * The baseline configuration of the system is reviewed and updated when system components are installed or upgraded. | Inherited  Partially Inherited |
| 13 | CM-7 | Least Functionality | * The system is configured to provide only CSP-defined mission-essential capabilities. * The use of CSP-defined functions, ports, protocols, software, and services is prohibited or restricted. | Inherited  Partially Inherited |
| 14 | IA-2 | Identification and Authentication (Organizational Users) | * Organizational users are uniquely identified and authenticated. * The unique identification of authenticated organizational users is associated with processes acting on behalf of those users. * The implementation of all control enhancements that specify multifactor authentication adhere to the Digital Identity Guidelines specified in NIST Special Publication 800-63B. * The multi-factor authentication implemented is phishing-resistant. * All uses of encrypted virtual private networks meet all applicable Federal requirements and architecture, dataflow, and security and privacy controls must be documented, assessed, and authorized to operate. | Inherited  Partially Inherited |
| 15 | IA-4 | Identifier Management | * System identifiers are managed by receiving authorization from at a minimum, the ISSO (or similar role within the organization) to assign to an individual, group, role, or device identifier. * System identifiers are managed by selecting an identifier that identifies an individual, group, role, service, or device. * System identifiers are managed by assigning the identifier to the intended individual, group, role, service, or device. * System identifiers are managed by preventing reuse of identifiers for at least two (2) years. | Inherited  Partially Inherited |
| 16 | IA-5 | Authenticator Management | * System authenticators are managed through the verification of the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution. * Authenticators are compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 3. Link <https://pages.nist.gov/800-63-3> * Authentication assertions are encrypted when passed through third parties, such as a browser. System authenticators are managed through the establishment of initial authenticator content for any authenticators issued by the organization. * System authenticators are managed to ensure that authenticators have sufficient strength of mechanism for their intended use. * System authenticators are managed through the establishment and implementation of administrative procedures for initial authenticator distribution; lost, compromised, or damaged authenticators; and the revocation of authenticators. * System authenticators are managed through the change of default authenticators prior to first use. * System authenticators are managed through the change or refreshment of authenticators CSP-defined time period by authenticator; CSP-defined events or when organization-defined events occur. * System authenticators are managed through the protection of authenticator content from unauthorized disclosure and modification. * System authenticators are managed through the requirement for individuals to take specific controls to protect authenticators. * System authenticators are managed through the requirement for devices to implement specific controls to protect authenticators. * System authenticators are managed through the change of authenticators for group or role accounts when membership to those accounts changes. | Inherited  Partially Inherited |
| 1 | IA-5 (1) | Authenticator Management | * For password-based authentication, a list of commonly used, expected, or compromised passwords is maintained and updated (and when organizational passwords are suspected to have been compromised directly or indirectly.) * Password policies are compliant with NIST SP 800-63B for all memorized, lookup, out-of-band, or One-Time-Passwords (OTP). Password policies do not enforce special character or minimum password rotation requirements for memorized secrets of users. * For password-based authentication when passwords are created or updated by users, the passwords are verified not to be found on the list of commonly used, expected, or compromised passwords above. * For password-based authentication, passwords are only transmitted over cryptographically protected channels. * For password-based authentication, passwords are stored using an approved salted key derivation function. * The CSP’s use of cryptography is compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.) * For password-based authentication, immediate selection of a new password is required upon account recovery. * For password-based authentication, user selection of long passwords and passphrases is allowed, including spaces and all printable characters. * For password-based authentication, automated tools are employed to assist the user in selecting strong password authenticators. * For password-based authentication, CSP-defined composition and complexity rules are enforced. | Inherited  Partially Inherited |
| 18 | IA-8 | Identification and Authentication (Non-organizational Users) | * Non-organizational users or processes acting on behalf of non-organizational users are uniquely identified and authenticated. | Inherited  Partially Inherited |
| 19. | IA-8 (4) | Identification and Authentication (Non-organizational Users) | * There is conformance with CSP-defined identity management profiles for identity management. | Inherited  Partially Inherited |
| 20 | IA-11 | Re-authentication | * Users are required to re-authenticate in accordance with NIST SP 800-63B. | Inherited  Partially Inherited |
| 21 | IR-2 | Incident Response Training | * Incident response training is provided to system users consistent with assigned roles and responsibilities within ten (10) days for privileged users, thirty (30) days for incident response roles of assuming an incident response role or responsibility or acquiring system access. * Incident response training is provided to system users consistent with assigned roles and responsibilities when required by system changes. * Incident response training is provided to system users consistent with assigned roles and responsibilities at least annually. * Incident response training content is reviewed and updated within the at least annually. * Incident response training content is reviewed and updated following CSP-defined events. | Inherited  Partially Inherited |
| 22. | IR-5 | Incident Monitoring | * Incidents are tracked and documented. | Inherited  Partially Inherited |
| 23 | IR-7 | Incident Response Assistance | * An incident response support resource, integral to the organizational incident response capability, is provided. * The incident response support resource offers advice and assistance to users of the system for the response and reporting of incidents. | Inherited  Partially Inherited |
| 24 | IR-8 | Incident Response Plan | * An incident response plan is developed 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 with regard 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  -addresses the sharing of incident information  -is reviewed and approved by CSP-defined personnel or roles; at least annually; CSP-defined entities, personnel, and/or roles within the organization-defined frequency  -explicitly designates responsibility for incident response to organization-defined entities, personnel, and/or roles.   * Copies of the incident response plan are distributed to a defined list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. * The incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing. * Incident response plan changes are communicated A list of incident response personnel (identified by name and/or by role) and organizational elements is defined. The incident response list includes designated FedRAMP personnel. * The incident response plan is protected from unauthorized disclosure and modification. | Inherited  Partially Inherited |
| 25 | MA-4 | Nonlocal Maintenance | * Nonlocal maintenance and diagnostic activities are approved and monitored. * The use of nonlocal maintenance and diagnostic tools are allowed only as consistent with organizational policy. * The use of nonlocal maintenance and diagnostic tools are documented in the security plan for the system. * Strong authentication is employed in the establishment of nonlocal maintenance and diagnostic sessions. * Records for nonlocal maintenance and diagnostic activities are maintained. * Session and network connections are terminated when nonlocal maintenance is completed. | Inherited  Partially Inherited |
| 26. | PL-4 | Rules of Behavior | * Rules that describe responsibilities and expected behavior for information and system usage, security, and privacy are established for and provided to individuals requiring access to the system. * Before authorizing access to information and the system, a documented acknowledgement from such individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received. * Rules of behavior are reviewed and updated at least every three (3) years. * Individuals who have acknowledged a previous version of the rules of behavior are required to read and reacknowledge at least annually and when the rules are revised or changed. | Inherited  Partially Inherited |
| 27 | PL-4(1) | Rules of Behavior | * The rules of behavior include restrictions on the use of social media, social networking sites, and external sites/applications. * The rules of behavior include restrictions on posting organizational information on public websites. * The rules of behavior include restrictions on the use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications. | Inherited  Partially Inherited |
| 28 | PL-10 | Baseline Selection | * The appropriate control baseline for the system is selected. | Inherited  Partially Inherited |
| 29. | PL-11 | Baseline Tailoring | * The selected control baseline is tailored by applying specified tailoring actions. | Inherited  Partially Inherited |
| 30 | PS-4 | Personnel Termination | * Upon termination of individual employment, system access is disabled within four (4) hours. * Upon termination of individual employment, any authenticators and credentials are terminated or revoked. * Upon termination of individual employment, exit interviews that include a discussion of CSP-defined information security topics are conducted. * Upon termination of individual employment, all security-related organizational system-related property is retrieved. * Upon termination of individual employment, access to organizational information and systems formerly controlled by the terminated individual are retained. | Inherited  Partially Inherited |
| 31. | PS-5 | Personnel Transfer | * The ongoing operational need for current logical and physical access authorizations to systems and facilities are reviewed and confirmed when individuals are reassigned or transferred to other positions within the organization. * CSP-defined transfer or reassignment actions; twenty-four (24) hours are initiated within organization-defined time period following the formal transfer action. * Access authorization is modified as needed to correspond with any changes in operational need due to reassignment or transfer. * Access control personnel responsible for the system are notified within twenty-four (24) hours. | Inherited  Partially Inherited |
| 32 | PS-6 | Access Agreements | * Access agreements are developed and documented for organizational systems. * The access agreements are reviewed and updated at least annually. * Individuals requiring access to organizational information and systems sign appropriate access agreements prior to being granted access. * Individuals requiring access to organizational information and systems re-sign access agreements to maintain access to organizational systems when access agreements have been updated or at least annually and any time there is a change to the user's level of access. | Inherited  Partially Inherited |
| 33 | PS-7 | External Personnel Security | * Personnel security requirements are established, including security roles and responsibilities for external providers. * External providers are required to comply with personnel security policies and procedures established by the organization. * Personnel security requirements are documented. * External providers are required to notify access control personnel responsible for the system and/or facilities, as appropriate; within twenty-four (24) hours of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges or who have system privileges within organization-defined time period. * Provider compliance with personnel security requirements is monitored. | Inherited  Partially Inherited |
| 34 | PS-8 | Personnel Sanctions | * A formal sanctions process is employed for individuals failing to comply with established information security and privacy policies and procedures. * At a minimum, the ISSO and/or similar role within the organization; CSP-defined time period is/are notified within organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. | Inherited  Partially Inherited |
| 35 | PS-9 | Position Descriptions | * Security and privacy roles and responsibilities are incorporated into organizational position descriptions. | Inherited  Partially Inherited |
| 36 | RA-3(1) | Risk Assessment | * Supply chain risks associated with CSP-defined systems, system components, and system services are assessed. * The supply chain risk assessment is updated within the CSP-defined frequency, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain. | Inherited  Partially Inherited |
| 37 | SA-2 | Allocation of Resources | * A security plan for the system is developed that is:   -consistent with the organization's enterprise architecture  -explicitly defines the constituent system components  -describes the operational context of the system in terms of mission and business processes.   * The high-level privacy requirements for the system or system service are determined in mission and business process planning. * The resources required to protect the system or system service are determined and documented as part of the organizational capital planning and investment control process. * The resources required to protect the system or system service are allocated as part of the organizational capital planning and investment control process. * A discrete line item for information security is established in organizational programming and budgeting documentation. * A discrete line item for privacy is established in organizational programming and budgeting documentation. | Inherited  Partially Inherited |
| 38 | SA-3 | System Development Life Cycle | * The system is acquired, developed, and managed using a CSP-defined system development life cycle that incorporates information security considerations. * The system is acquired, developed, and managed using a CSP-defined system development life cycle that incorporates privacy considerations. * Information security roles and responsibilities are defined and documented throughout the system development life cycle. * Privacy roles and responsibilities are defined and documented throughout the system development life cycle. * Individuals with information security roles and responsibilities are identified. * Individuals with privacy roles and responsibilities are identified. * Organizational information security risk management processes are integrated into system development life cycle activities. * Organizational privacy risk management processes are integrated into system development life cycle activities. | Inherited  Partially Inherited |
| 39 | SA-4 | Acquisition Process | * The following are included explicitly or by reference in the acquisition contract for the system, system component, or system service:   -security functional requirements, descriptions, and criteria  -security assurance requirements, descriptions, and criteria  -controls needed to satisfy the security requirements, descriptions, and criteria.   * The following are included explicitly or by reference in the acquisition contract for the system, system component, or system service:   -privacy functional requirements, descriptions, and criteria  -privacy assurance requirements, descriptions, and criteria  -controls needed to satisfy the privacy requirements, descriptions, and criteria.   * Strength of mechanism requirements, descriptions, and criteria are included explicitly or by reference in the acquisition contract for the system, system component, or system service. * Security and privacy documentation requirements, descriptions, and criteria are included explicitly or by reference in the acquisition contract for the system, system component, or system service. * Requirements for protecting security and privacy documentation, descriptions, and criteria are included explicitly or by reference in the acquisition contract for the system, system component, or system service. * The description of the system development environment and environment in which the system is intended to operate, requirements, and criteria are included explicitly or by reference in the acquisition contract for the system, system component, or system service. * The allocation of responsibility or identification of parties responsible for the following are included explicitly or by reference in the acquisition contract for the system, system component, or system service:   -information security requirements, descriptions, and criteria  -privacy requirements, descriptions, and criteria  -supply chain risk management requirements, description, and criteria.   * Acceptance criteria requirements and descriptions are included explicitly or by reference in the acquisition contract for the system, system component, or system service. * The CSP complies with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process). | Inherited  Partially Inherited |
| 40 | SA-4 (10) | Acquisition Process | * Only information technology products on the FIPS 201-approved products list for the personal identity verification (PIV) capability implemented within organizational systems are employed. | Inherited  Partially Inherited |
| 41. | SA-5 | System Documentation | * Administrator documentation for the system, system component, or system service that describes the following is obtained or developed:   -secure configuration  -secure installation  -secure operation.   * Administrator documentation for the system, system component, or system service that describes the following is obtained or developed:   -effective use of security functions and mechanisms  -effective maintenance of security functions and mechanisms.   * Administrator documentation for the system, system component, or system service that describes the following is obtained or developed:   -effective use of privacy functions and mechanisms  -effective maintenance of privacy functions and mechanisms.   * Administrator documentation for the system, system component, or system service that describes known vulnerabilities regarding the configuration and use of administrative or privileged functions is obtained or developed. * User documentation for the system, system component, or system service that describes user-accessible security functions and mechanisms, and how to effectively use them is obtained or developed. * User documentation for the system, system component, or system service that describes user-accessible privacy functions and mechanisms, and how to effectively use them is obtained or developed. * User documentation for the system, system component, or system service that describes methods for user interaction which enable individuals to use the system, component, or service in a more secure manner is obtained or developed. * User documentation for the system, system component, or system service that describes methods for user interaction which enable individuals to use the system, component, or service to protect individual privacy is obtained or developed. * User documentation for the system, system component, or system service that describes user responsibilities for maintaining the security of the system, component, or service is obtained or developed. * User documentation for the system, system component, or system service that describes user responsibilities for maintaining the privacy of individuals is obtained or developed. * Attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent is documented. * After attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent, CSP-defined actions are taken in response. * Documentation is distributed to at a minimum, the ISSO (or similar role within the organization). | Inherited  Partially Inherited |
| 42 | SA-8 | Security and Privacy Engineering Principles | * CSP-defined systems security engineering principles are applied in the specification, design, and development of the system and system components. * CSP-defined systems security engineering principles are applied in the implementation and modification of the system and system components. * CSP-defined privacy engineering principles are applied in the specification, design, and development of the system and system components. * CSP-defined privacy engineering principles are applied in the implementation and modification of the system and system components. | Inherited  Partially Inherited |
| 43 | SC-20 | Secure Name/Address Resolution Service (Authoritative Source) | * Additional data origin authentication and integrity verification artifacts are provided along with the authoritative name resolution data that the system returns in response to external name/address resolution queries. * The means to indicate the security status of child zones (and if the child supports secure resolution services) is provided when operating as part of a distributed, hierarchical namespace. * The means to enable verification of a chain of trust among parent and child domains when operating as part of a distributed, hierarchical namespace is provided. * Authoritative DNS servers are geolocated in accordance with SA-9 (5). | Inherited  Partially Inherited |
| 44 | SC-21 | Secure Name/Address Resolution Service (Recursive or Caching Resolver) | * Data origin authentication and integrity verification is requested and performed for the name/address resolution responses that the system receives from authoritative sources. * Internal recursive DNS servers are located inside an authorized environment. * DNSSEC resolution to access a component inside the boundary is excluded. | Inherited  Partially Inherited |
| 45 | SC-22 | Architecture and Provisioning for Name/Address Resolution Service | * The systems that collectively provide name/address resolution services for an organization are fault-tolerant, implement internal role separation and implement external role separation. | Inherited  Partially Inherited |
| 46 | SC-39 | Process Isolation | * A separate execution domain is maintained for each executing system process. | Inherited  Partially Inherited |
| 47 | SI-5 | Security Alerts, Advisories, and Directives | * System security alerts, advisories, and directives are received from US-CERT and Cybersecurity and Infrastructure Security Agency (CISA) directives on an ongoing basis. * The CSP addresses the CISA Emergency and Binding Operational Directives applicable to their cloud service offering per FedRAMP guidance. This includes listing the applicable directives and stating compliance status. * Internal security alerts, advisories, and directives are generated as deemed necessary. * Security alerts, advisories, and directives are disseminated to include system security personnel and administrators with configuration/patch-management responsibilities; organization-defined elements; organization-defined external organizations. * Security directives are implemented in accordance with established time frames or if the issuing organization is notified of the degree of noncompliance. | Inherited  Partially Inherited |
| 48. | SI-12 | Information Management and Retention | * Information and information output within the system is managed and retained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | Inherited  Partially Inherited |
| 49 | SR-2 | Supply Chain Risk Management Plan | * A plan for managing supply chain risks is developed. * The supply chain risk management plan addresses risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operation and disposal of CSP-defined systems, system components, or system services. * The supply chain risk management plan is reviewed and updated at least annually or as required to address threat, organizational, or environmental changes. * The supply chain risk management plan is protected from unauthorized disclosure and modification. | Inherited  Partially Inherited |
| 50 | SR-2(1) | Supply Chain Risk Management Plan | * A supply chain risk management team consisting of CSP-defined personnel, roles, and responsibilities; CSP-defined supply chain risk management activities is established to lead and support organization-defined supply chain risk management activities. | Inherited  Partially Inherited |
| 51 | SR-3 | Supply Chain Controls and Processes | * A process or processes is/are established to identify and address weaknesses or deficiencies in the supply chain elements and processes of see additional FedRAMP requirements / guidance. * The CSP documents and maintains the supply chain custody, including replacement devices, to ensure the integrity of the devices before being introduced to the boundary. * The process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of CSP-defined system or system component; CSP-defined supply chain personnel is/are coordinated with organization-defined supply chain personnel. * CSP-defined supply chain controls are employed to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events. * The selected and implemented supply chain processes and controls are documented in CSP-defined security and privacy plans; supply chain security and privacy plans; supply chain risk management plan. | Inherited  Partially Inherited |
| 52. | SR-5 | Acquisition Strategies, Tools, and Methods | * CSP-defined strategies, tools, and methods are employed to protect, identify, and mitigate against supply chain risks. | Inherited  Partially Inherited |
| 53 | SR-8 | Notification Agreements | * Agreements and procedures are established with entities involved in the supply chain for the system, system components, or system service for notification of supply chain compromises and results of assessment or audits. * The CSP ensures and documents how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities. | Inherited  Partially Inherited |
| 54 | SR-10 | Inspection of Systems or Components | * CSP-defined systems or system components are inspected at random; at organization-defined frequency; upon organization-defined indications of need for inspection are inspected at random; at organization-defined frequency; upon organization-defined indications of need for inspection to detect tampering. | Inherited  Partially Inherited |
| 55 | SR-11 | Component Authenticity | * Anti-counterfeit policy and anti-counterfeit procedures are developed and implemented. * The anti-counterfeit procedures include the means to detect and prevent counterfeit components entering the system. * Counterfeit system components are reported to see additional FedRAMP requirements / guidance. * The CSP ensures that their supply chain vendors provide authenticity of software and patches and the vendor must have a plan to protect the development pipeline. | Inherited  Partially Inherited |
| 56 | SR-11(1) | Component Authenticity | * CSP-defined personnel or roles are trained to detect counterfeit system components (including hardware, software, and firmware). | Inherited  Partially Inherited |
| 57 | SR-11(2) | Component Authenticity | * Configuration control over all system components and serviced or repaired all system components awaiting service or repair is maintained. | Inherited  Partially Inherited |
| 58 | SR-12 | Component Disposal | * CSP-defined data, documentation, tools, or system component; CSP-defined techniques and methods are disposed of using organization-defined techniques and methods. | Inherited  Partially Inherited |