|  |
| --- |
| NILES System Security Plan (SSP) Template  Service Provider Name  Information System Name  Version #  Version Date |



Instruction: This template contains a number of features to facilitate data entry. As you go through the template entering data, you will see prompts for you to enter different types of data.

Repeatable Field

Some multiple-occurring data fields have been linked together and you need only enter the data once. Enter the data once; then click outside the data entry field and all occurrences of that field will be populated. For example, when you see “Information System Abbreviation” and replace it with your system abbreviation, all instances of the abbreviation throughout the document will be replaced with the value you entered. This document contains the following repeatable fields:

SP Name

Information System Name

Version Number

Version Date

Information System Abbreviation

If you find a data field from the above list that has not populated, then press the F9 key to refresh the data. If you make a change to one of the above data fields, you may also have to press the F9 key to refresh the data throughout the document. Remember to save the document after refreshes. The one exception to the repeatable fields is information system names for Company or leveraged authorizations that are identified as “Leveraged information system name:

Date Selection

Data fields that must contain a date will present a date selection menu.

Item Choice

Data fields that have a limited number of value choices will present a selection list.

Number Entry

Data fields that must have numeric values display “number.”

Text Entry

Many data fields, particularly in tables, that can contain any text display “Enter text” or “Click here to enter text.”

Delete this instruction from your final version of this document.

System Security Plan

Prepared by

|  |  |  |
| --- | --- | --- |
| **Identification of Organization that Prepared this Document** | | |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Prepared for

|  |  |  |
| --- | --- | --- |
| **Identification of `Service Provider** | | |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Template Revision History

|  |  |
| --- | --- |
| **Date** | **Description** |
| 9/30/2016 | Original publication |
| 10/21/2016 | Removed tables in Sec 15.12 Company Laws and Regulations  Removed revision history tables in all of Sec 15  Removed Acronyms - see Company Master Acronyms and Glossary resource document  Added PTA to Sec 15.4 PTA and PIA  Added E-Authentication to Sec 15.3  Added FIPs to Sec 15.10 FIPS 199  Changed Inventory instruction and guidance Sec 10 and Attachment 13  Removed chapter numbers from Attachments  Removed 3 questions from Sec 2.3 E-Authentication Determination |
| 3/6/2017 | Renamed document from "Company System Security Plan (SSP) Low Baseline Master Template to "Company System Security Plan (SSP) Low Baseline Template" |
| 6/6/2017 | Updated logo |
| 8/28/2018 | Revised controls for language consistency, updated section 2.3 and Attachment 3, added guidance to SA -9, updated requirements in RA-5 |
| 5/18/2021 | Revised SA-4 Additional Company Requirements and Guidance |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version of SSP | Author |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

How to contact us

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

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

Instruction: The System Security Plan is the main document in which the Service Provider (SP) describes all the security controls in use on the information system and their implementation.

This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.

This document is intended to be used by service providers who are applying for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) or an Agency Authorization to Operate (ATO) through the Federal Risk and Authorization Management Program (Company).  
  
In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from 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 SP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.

Note that “-1” Controls (AC-1, AU-1, SC-1, etc.)\* cannot be inherited and must be described in some way by the service provider.  
\*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) 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.

For System as a Service (SaaS) and Platform as a Service (PaaS) systems that are inheriting controls from an Infrastructure as a Service (IaaS) (or anything lower in the stack), the “inherited” check box must be checked and the implementation description must simply say “inherited.” Company reviewers will determine whether the control-set is appropriate or not.

In Section 13, the National Institute of Standards and Technology (NIST) term "organization defined" must be interpreted as being the SP's responsibility unless otherwise indicated. In some cases, the JAB has chosen to define or provide parameters, in others they have left the decision up to the SP.

Delete this instruction from your final version of this document.

TABLE OF CONTENTS

[1. Information System Name/Title 1](#_Toc140101543)

[2. Information System Categorization 1](#_Toc140101544)

[2.1. Information Types 1](#_Toc140101545)

[2.2. Security Objectives Categorization (FIPS 199) 3](#_Toc140101546)

[2.3. Digital Identity Determination 4](#_Toc140101547)

[3. Information System Owner 4](#_Toc140101548)

[4. Authorizing Official 4](#_Toc140101549)

[5. Other Designated Contacts 5](#_Toc140101550)

[6. Assignment of Security Responsibility 6](#_Toc140101551)

[7. Information System Operational Status 7](#_Toc140101552)

[8. Information System Type 7](#_Toc140101553)

[8.1. Service Models 7](#_Toc140101554)

[8.2. Deployment Models 8](#_Toc140101555)

[8.3. Leveraged Authorizations 9](#_Toc140101556)

[9. General System Description 9](#_Toc140101557)

[9.1. System Function or Purpose 9](#_Toc140101558)

[9.2. Information System Components and Boundaries 10](#_Toc140101559)

[9.3. Types of Users 11](#_Toc140101560)

[9.4. Network Architecture 12](#_Toc140101561)

[10. System Environment And Inventory 12](#_Toc140101562)

[10.1. Data Flow 14](#_Toc140101563)

[10.2. Ports, Protocols and Services 15](#_Toc140101564)

[11. System Interconnections 16](#_Toc140101565)

[12. Laws, Regulations, Standards and Guidance 18](#_Toc140101566)

[12.1. Applicable Laws and Regulations 18](#_Toc140101567)

[12.2. Applicable Standards and Guidance 18](#_Toc140101568)

[13. Minimum Security Controls 19](#_Toc140101569)

[13.1. Access Control (AC) 27](#_Toc140101570)

[AC-1 Access Control Policy and Procedures Requirements (L) (M) 27](#_Toc140101571)

[AC-2 Account Management (L) (M) 28](#_Toc140101572)

[AC-3 Access Enforcement (L) (M) (H) 29](#_Toc140101573)

[AC-7 Unsuccessful Login Attempts (L) (M) 30](#_Toc140101574)

[AC-8 System Use Notification (L) (M) (H) 31](#_Toc140101575)

[AC-14 Permitted Actions without Identification or Authentication (L) (M) (H) 34](#_Toc140101576)

[AC-17 Remote Access (L) (M) (H) 34](#_Toc140101577)

[AC-18 Wireless Access Restrictions (L) (M) (H) 35](#_Toc140101578)

[AC-19 Access Control for Portable and Mobile Systems (L) (M) (H) 36](#_Toc140101579)

[AC-20 Use of External Information Systems (L) (M) (H) 37](#_Toc140101580)

[AC-22 Publicly Accessible Content (L) (M) (H) 38](#_Toc140101581)

[13.2. Awareness and Training (AT) 39](#_Toc140101582)

[AT-1 Security Awareness and Training Policy and Procedures (L) (M) 39](#_Toc140101583)

[AT-2 Security Awareness (L) (M) (H) 40](#_Toc140101584)

[AT-3 Role-Based Security Training (L) (M) (H) 40](#_Toc140101585)

[AT-4 Security Training Records (L) (M) 41](#_Toc140101586)

[13.3. Audit and Accountability (AU) 42](#_Toc140101587)

[AU-1 Audit and Accountability Policy and Procedures (L) (M) 42](#_Toc140101588)

[AU-2 Audit Events (L) (M) (H) 43](#_Toc140101589)

[AU-3 Content of Audit Records (L) (M) (H) 44](#_Toc140101590)

[AU-4 Audit Storage Capacity (L) (M) (H) 45](#_Toc140101591)

[AU-5 Response to Audit Processing Failures (L) (M) (H) 46](#_Toc140101592)

[AU-6 Audit Review, Analysis, and Reporting (L) (M) (H) 46](#_Toc140101593)

[AU-8 Time Stamps (L) (M) (H) 47](#_Toc140101594)

[AU-9 Protection of Audit Information (L) (M) (H) 48](#_Toc140101595)

[AU-11 Audit Record Retention (L) (M) 49](#_Toc140101596)

[AU-12 Audit Generation (L) (M) (H) 50](#_Toc140101597)

[13.4. Security Assessment and Authorization (CA) 51](#_Toc140101598)

[CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M) 51](#_Toc140101599)

[CA-2 Security Assessments (L) (M) (H) 52](#_Toc140101600)

[CA-2 (1) Control Enhancement (L) (M) (H) 53](#_Toc140101601)

[CA-3 System Interconnections (L) (M) (H) 54](#_Toc140101602)

[CA-5 Plan of Action and Milestones (L) (M) (H) 55](#_Toc140101603)

[CA-6 Security Authorization (L) (M) (H) 56](#_Toc140101604)

[CA-7 Continuous Monitoring (L) (M) (H) 57](#_Toc140101605)

[CA-9 Internal System Connections (L) (M) (H) 59](#_Toc140101606)

[13.5. Configuration Management (CM) 60](#_Toc140101607)

[CM-1 Configuration Management Policies and Procedures (L) (M) 60](#_Toc140101608)

[CM-2 Baseline Configuration (L) (M) (H) 61](#_Toc140101609)

[CM-4 Security Impact Analysis (L) (M) (H) 62](#_Toc140101610)

[CM-6 Configuration Settings (L) (M) (H) 63](#_Toc140101611)

[CM-7 Least Functionality (L) (M) (H) 64](#_Toc140101612)

[CM-8 Information System Component Inventory (L) (M) (H) 65](#_Toc140101613)

[CM-10 Software Usage Restrictions (L) (M) (H) 66](#_Toc140101614)

[CM-11 User-Installed Software (L) (M) (H) 67](#_Toc140101615)

[13.6. Contingency Planning (CP) 68](#_Toc140101616)

[CP-1 Contingency Planning Policy and Procedures (L) (M) 68](#_Toc140101617)

[CP-2 Contingency Plan (L) (M) (H) 69](#_Toc140101618)

[CP-3 Contingency Training (L) (M) (H) 71](#_Toc140101619)

[CP-4 Contingency Plan Testing (L) 72](#_Toc140101620)

[CP-9 Information System Backup (L) (M) (H) 73](#_Toc140101621)

[CP-10 Information System Recovery and Reconstitution (L) (M) (H) 74](#_Toc140101622)

[13.7. Identification and Authentication (IA) 75](#_Toc140101623)

[IA-1 Identification and Authentication Policy and Procedures (L) (M) 75](#_Toc140101624)

[IA-2 User Identification and Authentication (L) (M) (H) 76](#_Toc140101625)

[IA-2 (1) Control Enhancement (L) (M) (H) 76](#_Toc140101626)

[IA-2 (12) Control Enhancement (L) (M) (H) 77](#_Toc140101627)

[IA-4 Identifier Management (L) (M) 78](#_Toc140101628)

[IA-5 Authenticator Management (L) (M) 79](#_Toc140101629)

[IA-5 (1) Control Enhancement (L) (M) 81](#_Toc140101630)

[IA-5 (11) Control Enhancement (L) (M) (H) 82](#_Toc140101631)

[IA-6 Authenticator Feedback (L) (M) (H) 83](#_Toc140101632)

[IA-7 Cryptographic Module Authentication (L) (M) (H) 83](#_Toc140101633)

[IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H) 84](#_Toc140101634)

[IA-8 (1) Control Enhancement (L) (M) (H) 85](#_Toc140101635)

[IA-8 (2) Control Enhancement (L) (M) (H) 85](#_Toc140101636)

[IA-8 (3) Control Enhancement (L) (M) (H) 86](#_Toc140101637)

[IA-8 (4) Control Enhancement (L) (M) (H) 86](#_Toc140101638)

[13.8. Incident Response (IR) 87](#_Toc140101639)

[IR-1 Incident Response Policy and Procedures (L) (M) 87](#_Toc140101640)

[IR-2 Incident Response Training (L) (M) 88](#_Toc140101641)

[IR-4 Incident Handling (L) (M) (H) 89](#_Toc140101642)

[IR-5 Incident Monitoring (L) (M) (H) 90](#_Toc140101643)

[IR-6 Incident Reporting (L) (M) (H) 91](#_Toc140101644)

[IR-7 Incident Response Assistance (L) (M) (H) 92](#_Toc140101645)

[IR-8 Incident Response Plan (L) (M) (H) 92](#_Toc140101646)

[13.9. Maintenance (MA) 94](#_Toc140101647)

[MA-1 System Maintenance Policy and Procedures (L) (M) 94](#_Toc140101648)

[MA-2 Controlled Maintenance (L) (M) (H) 95](#_Toc140101649)

[MA-4 Remote Maintenance (L) (M) (H) 96](#_Toc140101650)

[MA-5 Maintenance Personnel (L) (M) (H) 97](#_Toc140101651)

[13.10. Media Protection (MP) 98](#_Toc140101652)

[MP-1 Media Protection Policy and Procedures (L) (M) 98](#_Toc140101653)

[MP-2 Media Access (L) (M) 99](#_Toc140101654)

[MP-6 Media Sanitization and Disposal (L) (M) 100](#_Toc140101655)

[MP-7 Media Use (L) (M) (H) 101](#_Toc140101656)

[13.11. Physical and Environmental Protection (PE) 102](#_Toc140101657)

[PE-1 Physical and Environmental Protection Policy and Procedures (L) (M) 102](#_Toc140101658)

[PE-2 Physical Access Authorizations (L) (M) 103](#_Toc140101659)

[PE-3 Physical Access Control (L) (M) (H) 104](#_Toc140101660)

[PE-6 Monitoring Physical Access (L) (M) (H) 105](#_Toc140101661)

[PE-8 Visitor Access Records (L) (M) (H) 106](#_Toc140101662)

[PE-12 Emergency Lighting (L) (M) (H) 107](#_Toc140101663)

[PE-13 Fire Protection (L) (M) (H) 108](#_Toc140101664)

[PE-14 Temperature and Humidity Controls (L) (M) (H) 108](#_Toc140101665)

[PE-15 Water Damage Protection (L) (M) (H) 109](#_Toc140101666)

[PE-16 Delivery and Removal (L) (M) (H) 110](#_Toc140101667)

[13.12. Planning (PL) 111](#_Toc140101668)

[PL-1 Security Planning Policy and Procedures (L) (M) 111](#_Toc140101669)

[PL-2 System Security Plan (L) (M) (H) 112](#_Toc140101670)

[PL-4 Rules of Behavior (L) (M) 113](#_Toc140101671)

[13.13. Personnel Security (PS) 114](#_Toc140101672)

[PS-1 Personnel Security Policy and Procedures (L) (M) 114](#_Toc140101673)

[PS-2 Position Categorization (L) (M) 115](#_Toc140101674)

[PS-3 Personnel Screening (L) (M) (H) 116](#_Toc140101675)

[PS-4 Personnel Termination (L) (M) 117](#_Toc140101676)

[PS-5 Personnel Transfer (L) (M) 118](#_Toc140101677)

[PS-6 Access Agreements (L) (M) 119](#_Toc140101678)

[PS-7 Third-Party Personnel Security (L) (M) 120](#_Toc140101679)

[PS-8 Personnel Sanctions (L) (M) 121](#_Toc140101680)

[13.14. Risk Assessment (RA) 122](#_Toc140101681)

[RA-1 Risk Assessment Policy and Procedures (L) (M) 122](#_Toc140101682)

[RA-2 Security Categorization (L) (M) (H) 123](#_Toc140101683)

[RA-3 Risk Assessment (L) (M) 124](#_Toc140101684)

[RA-5 Vulnerability Scanning (L) (M) (H) 126](#_Toc140101685)

[13.15. System and Services Acquisition (SA) 127](#_Toc140101686)

[SA-1 System and Services Acquisition Policy and Procedures (L) (M) 127](#_Toc140101687)

[SA-2 Allocation of Resources (L) (M) (H) 128](#_Toc140101688)

[SA-3 System Development Life Cycle (L) (M) (H) 129](#_Toc140101689)

[SA-4 Acquisitions Process (L) (M) (H) 130](#_Toc140101690)

[SA-5 Information System Documentation (L) (M) 131](#_Toc140101691)

[SA-9 External Information System Services (L) (M) (H) 133](#_Toc140101692)

[13.16. System and Communications Protection (SC) 134](#_Toc140101693)

[SC-1 System and Communications Protection Policy and Procedures (L) (M) 134](#_Toc140101694)

[SC-5 Denial of Service Protection (L) (M) (H) 135](#_Toc140101695)

[SC-7 Boundary Protection (L) (M) (H) 136](#_Toc140101696)

[SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 137](#_Toc140101697)

[SC-13 Use of Cryptography (L) (M) (H) 138](#_Toc140101698)

[SC-15 Collaborative Computing Devices (L) (M) (H) 138](#_Toc140101699)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 140](#_Toc140101700)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 141](#_Toc140101701)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 141](#_Toc140101702)

[SC-39 Process Isolation (L) (M) (H) 142](#_Toc140101703)

[13.17. System and Information Integrity (SI) 143](#_Toc140101704)

[SI-1 System and Information Integrity Policy and Procedures (L) (M) 143](#_Toc140101705)

[SI-2 Flaw Remediation (L) (M) (H) 144](#_Toc140101706)

[SI-3 Malicious Code Protection (L) (M) 145](#_Toc140101707)

[SI-4 Information System Monitoring (L) (M) (H) 146](#_Toc140101708)

[SI-5 Security Alerts & Advisories (L) (M) (H) 148](#_Toc140101709)

[SI-12 Information Output Handling and Retention (L) (M) (H) 149](#_Toc140101710)

[SI-16 Memory Protection (L) (M) (H) 149](#_Toc140101711)

[14. Acronyms 151](#_Toc140101712)

[Systems Security Plan Attachments 152](#_Toc140101713)

[15. Attachments 152](#_Toc140101714)

[Attachment 1 Information Security Policies and Procedures 154](#_Toc140101715)

[Attachment 2 User Guide 155](#_Toc140101716)

[Attachment 3 Digital Identity Worksheet 156](#_Toc140101717)

[Introduction and Purpose 156](#_Toc140101718)

[Information System Name/Title 156](#_Toc140101719)

[Digital Identity Level Definitions 156](#_Toc140101720)

[Review Maximum Potential Impact Levels 157](#_Toc140101721)

[Digital Identity Level Selection 158](#_Toc140101722)

[Attachment 4 PTA / PIA 159](#_Toc140101723)

[Privacy Overview and Point of Contact (POC) 159](#_Toc140101724)

[Applicable Laws and Regulations 159](#_Toc140101725)

[Applicable Standards and Guidance 160](#_Toc140101726)

[Personally Identifiable Information (PII) 160](#_Toc140101727)

[Privacy Threshold Analysis 161](#_Toc140101728)

[Qualifying Questions 161](#_Toc140101729)

[Designation 161](#_Toc140101730)

[Attachment 5 Rules of Behavior 162](#_Toc140101731)

[Attachment 6 Information System Contingency Plan 163](#_Toc140101732)

[Attachment 7 Configuration Management Plan 164](#_Toc140101733)

[Attachment 8 Incident Response Plan 165](#_Toc140101734)

[Attachment 9 CIS Workbook 166](#_Toc140101735)

[Attachment 10 FIPS 199 167](#_Toc140101736)

[Introduction and Purpose 167](#_Toc140101737)

[Scope 167](#_Toc140101738)

[System Description 167](#_Toc140101739)

[Methodology 168](#_Toc140101740)

[Attachment 11 Separation of Duties Matrix 170](#_Toc140101741)

[Attachment 12 Company Laws and Regulations 171](#_Toc140101742)

[Attachment 13 Company Inventory Workbook 172](#_Toc140101743)

List of Figures

[Figure 9‑1. Authorization Boundary Diagram 10](#_Toc523079035)

[Figure 9‑2. Network Diagram 12](#_Toc523079036)

[Figure 10‑1. Data Flow Diagram 13](#_Toc523079037)

List of Tables

[Table 1‑1. Information System Name and Title 1](#_Toc523079038)

[Table 2‑1. Security Categorization 1](#_Toc523079039)

[Table 2‑2. Sensitivity Categorization of Information Types 3](#_Toc523079040)

[Table 2‑3. Security Impact Level 3](#_Toc523079041)

[Table 2‑4. Baseline Security Configuration 3](#_Toc523079042)

[Table 3‑1. Information System Owner 4](#_Toc523079043)

[Table 5‑1. Information System Management Point of Contact 5](#_Toc523079044)

[Table 5‑2. Information System Technical Point of Contact 5](#_Toc523079045)

[Table 6‑1. SP Name Internal ISSO (or Equivalent) Point of Contact 6](#_Toc523079046)

[Table 6‑2. AO Point of Contact 6](#_Toc523079047)

[Table 7‑1. System Status 7](#_Toc523079048)

[Table 8‑1. Service Layers Represented in this SSP 8](#_Toc523079049)

[Table 8‑2. Deployment Model Represented in this SSP 8](#_Toc523079050)

[Table 8‑3. Leveraged Authorizations 9](#_Toc523079051)

[Table 9‑1. Personnel Roles and Privileges 11](#_Toc523079052)

[Table 10‑1. Ports, Protocols and Services 14](#_Toc523079053)

[Table 11‑1. System Interconnections 15](#_Toc523079054)

[Table 12‑1. Information System Name Laws and Regulations 17](#_Toc523079055)

[Table 12‑2. Information System Name Standards and Guidance 17](#_Toc523079056)

[Table 13‑1. Summary of Required Security Controls 18](#_Toc523079057)

[Table 13‑2. Control Origination and Definitions 25](#_Toc523079058)

[Table 13‑3. CA-3 Authorized Connections 53](#_Toc523079059)

[Table 15‑1. Names of Provided Attachments 151](#_Toc523079060)

[Table 15‑2. Information System Name and Title 155](#_Toc523079061)

[Table 15‑3. Mapping Company Levels to NIST SP 800-63-3 Levels 156](#_Toc523079062)

[Table 15‑4. Potential Impacts for Assurance Levels 157](#_Toc523079063)

[Table 15‑5. Digital Identity Level 157](#_Toc523079064)

[Table 15‑6. Information System Name Privacy POC 158](#_Toc523079065)

[Table 15‑7. Information System Name Laws and Regulations 159](#_Toc523079066)

[Table 15‑8. Information System Name Standards and Guidance 159](#_Toc523079067)

[Table 15‑9. SP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1 168](#_Toc523079068)

[Table 15‑10. Company Templates that Reference Company Laws and Regulations Standards and Guidance 170](#_Toc523079069)

System Security Plan Approvals

Service Provider Signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Service Provider | | SP Name | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Service Provider | | SP Name | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Service Provider | | SP Name | | |
|  | |  | | |

# Information System Name

This System Security Plan provides an overview of the security requirements for the Information System Name (NILES) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed, or stored by the NILES information system.

The security safeguards implemented for the Enter Information System Abbreviation system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

| Unique Identifier | Information System Name |
| --- | --- |
| M512-45 | Information System Name |

Table 1‑1. Information System Name

# Information System Categorization

The overall information system sensitivity categorization is recorded in Table 2‑1. Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: **Attachment 10, FIPS 199.**

|  |  |
| --- | --- |
| System Sensitivity Level: | Low (L) |

Table 2‑1. Security Categorization

## Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed and/or output from Enter Information System Abbreviation. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

The tables also identify the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is low if—

* The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
* A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is moderate if—

* The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
* A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is high if—

* The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
* A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

| Information Type | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| Debt Collection Information Type | C.2.5.1 | Moderate (M) | Low (L) | Low (L) |
| Proposal Development information type | C.2.7.3 | Moderate (M) | Low (L) | Low (L) |
| Reporting process information type | C.3.2.2. | Low (L) | Moderate (M) | High (H) |

## Table 2‑2. Sensitivity Categorization of Information Types

## Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2‑2. Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, default to the high-water mark for the Information Types as identified in Table 2‑3. Security Impact Level below.

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | Moderate (M) |
| Integrity | Moderate (M) |
| Availability | High (H) |

Table 2‑3. Security Impact Level

Through review and analysis, it has been determined that the baseline security categorization for the Enter Information System Abbreviation system is listed in the Table 2‑4. Baseline Security Configuration that follows.

|  |  |
| --- | --- |
| Enter Information System Abbreviation Security Categorization | High (H) |

Table 2‑4. Baseline Security Configuration

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

## Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Choose an item.

Additional digital identity information can be found in Section 15 Attachments Digital Identity Level Selection.

# Information System Owner

The following individual is identified as the system owner for this system.

| Information System Owner Information | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

Table 3‑1. Information System Owner

# Authorizing Official

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the Insert AO information as instructed above.

# Other Designated Contacts

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

| Information System Management Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

Table 5‑1. Information System Management Point of Contact

| Information System Technical Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

Table 5‑2. Information System Technical Point of Contact

| Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

# Assignment of Security Responsibility

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6‑1. SP Name Internal ISSO (or Equivalent) Point of Contact

| SP Name Internal ISSO (or Equivalent) Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

Table 6‑2. AO Point of Contact

|  |  |
| --- | --- |
| AO Point of Contact | |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

# Information System Operational Status

The system is currently in the life-cycle phase shown in Table 7‑1. System Status that follows. (Only operational systems can be granted an ATO).

| System Status | | |
| --- | --- | --- |
|  | Operational | The system is operating and in production. |
|  | Under Development | The system is being designed, developed, or implemented |
|  | Major Modification | The system is undergoing a major change, development, or transition. |
|  | Other | Explain: Click here to enter text. |

Table 7‑1. System Status

# Information System Type

The Enter Information System Abbreviation makes use of unique managed service provider architecture layer(s).

## Service Models

Information systems, particularly those based on architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a followed by specific questions to help the system owner determine the type of cloud.

|  |  |
| --- | --- |
| Question (Yes/No) | Conclusion |
| Does the system use virtual machines? | A no response means that system is most likely not a cloud. |
| Does the system have the ability to expand its capacity to meet customer demand? | A no response means that the system is most likely not a cloud. |
| Does the system allow the consumer to build anything other than servers? | A no response, means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS. |
| Does the system offer the ability to create databases? | A yes response means that the system is a PaaS. |
| Does the system offer various developer toolkits and APIs? | A yes response means that the system is a PaaS. |
| Does the system offer only applications that are available by obtaining a login? | A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS. |

The layers of the Enter Information System Abbreviation defined in this SSP are indicated in Table 8‑1. Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply.

Delete this and all other instructions from your final version of this document.

Table 8‑1. Service Layers Represented in this SSP

| Service Provider Architecture Layers | | |
| --- | --- | --- |
|  | Software as a Service (SaaS) | Major Application |
|  | Platform as a Service (PaaS) | Major Application |
|  | Infrastructure as a Service (IaaS) | General Support System |
|  | Other | Explain: Click here to enter text. |

Note: Refer to NIST SP 800-145 for information on computing architecture models.

## Deployment Models

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other Company Authorizations, are indicated in Table 8‑2. Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

Table 8‑2. Deployment Model Represented in this SSP

| Service Provider Deployment Model | | |
| --- | --- | --- |
|  | Public | Services and infrastructure supporting multiple organizations and agency clients |
|  | Private | Services and infrastructure dedicated to a specific organization/agency and no other clients |
|  | Government Only Community | Services and infrastructure shared by several organizations/agencies with same policy and compliance considerations |
|  | Hybrid | Explain: (e.g., Services and infrastructure that provides private for secured applications and data where required and public for other applications and data)  Click here to enter text. |

## Leveraged Authorizations

Instruction: The Company program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. If a lower level layer has been granted an Authorization and another higher level layer represented by this SSP plans to leverage a lower layer’s Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write “None” in the first column of the table that follows. Add as many rows as necessary in the table that follows.

Delete this and all other instructions from your final version of this document.

The Enter Information System Abbreviation Choose an item leverages a pre-existing Company Authorization. Company Authorizations leveraged by this Enter Information System Abbreviation are listed in Table 8‑3. Leveraged Authorizations that follows.

Table 8‑3. Leveraged Authorizations

| Leveraged Information System Name | Leveraged Service Provider Owner | Date Granted |
| --- | --- | --- |
| <Enter Leveraged information system name1> | <Enter service provider owner1> | <Date> |
| <Enter Leveraged information system name2> | <Enter service provider owner2> | <Date> |
| <Enter Leveraged information system name3> | <Enter service provider owner3> | <Date> |

# General System Description

This section includes a general description of NILES system.

## System Function or PurposDelete this and all other instructions from your final version of this document.

## Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system’s Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)].

**Additional Company Requirements and Guidance:**

**Guidance:** See the Company Documents page under Key Service Provider (SP) Documents> Company Authorization Boundary Guidance

[https://www.company.gov/documents/](https://www.fedramp.gov/documents/)

Delete this and all other instructions from your final version of this document.

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9‑1. Authorization Boundary Diagram below.

|  |
| --- |
|  |

Figure 9‑1. Authorization Boundary Diagram

## Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9‑1. Personnel Roles and Privileges that follows.

Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role type. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the SP service offering.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.

Delete this and all other instructions from your final version of this document.

Table 9‑1. Personnel Roles and Privileges

| Role | Internal or External | Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) | Sensitivity Level | Authorized Privileges | Functions Performed |
| --- | --- | --- | --- | --- | --- |
| UNIX System Administrator | Internal | PP | Moderate | Full administrative access (root) | Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups |
| Client Administrator | External | NP | N/A | Portal administration | Add/remote client users. Create, modify and delete client applications |
| Program Director | Internal | NLA | Limited | N/A | Reviews, approves and enforces policy |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

## Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.

Delete this and all other instructions from your final version of this document.

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9‑2. Network Diagram mapping the data flow between components.

The following Figure 9‑2. Network Diagram(s) provides a visual depiction of the system network components that constitute Enter Information System Abbreviation.

|  |
| --- |
|  |

Figure 9‑2. Network Diagram

# System Environment And Inventory

Directions for attaching the Company Inventory Workbook may be found in the following section: Attachment 13, Company Inventory Workbook.

Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g., production environment, test environment, staging or QA environments. Include the specific location of the alternate, backup and operational facilities.

In your description, also include a reference to Attachment 13, the system’s Integrated Inventory Workbook, which should provide a complete listing of the system’s components (operating systems/infrastructure, web applications/software, and databases). The Integrated Inventory Workbook should be maintained and updated monthly by the SP, as part of continuous monitoring efforts. Instructions for completing the Integrated Inventory Workbook are provided within the Integrated Inventory Workbook.

Delete this and all other instructions from your final version of this document.

## Data Flow

Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.

Delete this and all other instructions from your final version of this document.

The data flow in and out of the system boundaries is represented in Figure 10‑1. Data Flow Diagram below.

|  |
| --- |
|  |

Figure 10‑1. Data Flow Diagram

## Ports, Protocols and Services

The Table 10‑1. Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

Instruction: In the column labeled “Used By” please indicate the components of the information system that make use of the ports, protocols and services. In the column labeled “Purpose” indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing Company Authorization. Add more rows as needed.

Delete this and all other instructions from your final version of this document.

Table 10‑1. Ports, Protocols and Services

| Ports (TCP/UDP)\* | Protocols | Services | Purpose | Used By |
| --- | --- | --- | --- | --- |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |

\* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

# System Interconnections

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the SP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13‑3 CA-3 Authorized Connections.

**Additional Company Requirements and Guidance:**

**Guidance**: See the Company Documents page under Key Service Provider (SP) Documents> Company Authorization Boundary Guidance

[https://www.company.gov/documents/](https://www.fedramp.gov/documents/)

Delete this and all other instructions from your final version of this document.

Table 11‑1. System Interconnections below is consistent with Table 13‑3 CA-3 Authorized Connections.

Table 11‑1. System Interconnections

| SP\* IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)\*\* | Data Direction  (incoming, outgoing, or both) | Information Being Transmitted | Port or Circuit Numbers |
| --- | --- | --- | --- | --- | --- | --- |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |

\*Service Processor

\*\*Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

# Laws, Regulations, Standards and Guidance

A summary of Laws and Regulations is included in Attachment 12, Applicable Laws and Regulations

Table 12‑1. Information System Name Laws and Regulations includes additional laws and regulations specific to Information System Name.

Table 12‑1. Information System Name Laws and Regulations

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

## Applicable Standards and Guidance

The applicable Standards and Guidance be found on this web page: [Templates](https://www.fedramp.gov/templates)

Table 12‑2. Information System Name Standards and Guidance includes in this section any additional standards and guidance specific to Information System Name.

Table 12‑2. Information System Name Standards and Guidance

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

# Minimum Security Controls

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of Enter Information System Abbreviation are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional Company controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parentheses in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low, systems categorized as FIPS 199 Moderate use the controls designated as Moderate and systems categorized as FIPS 199 High use the controls designated as High. A summary of which security standards pertain to which sensitivity level is found in Table 13‑1. Summary of Required Security Controls that follows.

Table 13‑1. Summary of Required Security Controls

| ID | Control Description | Sensitivity Level | | |
| --- | --- | --- | --- | --- |
| Low | Moderate | High |
| AC | Access Control | | | |
| AC-1 | Access Control Policy and Procedures | AC-1 | AC-1 | AC-1 |
| AC-2 | Account Management | AC-2 | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12) | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13) |
| AC-3 | Access Enforcement | AC-3 | AC-3 | AC-3 |
| AC-4 | Information Flow Enforcement | Not Selected | AC-4 (21) | AC-4 (8) (21) |
| AC-5 | Separation of Duties | Not Selected | AC-5 | AC-5 |
| AC-6 | Least Privilege | Not Selected | AC-6 (1) (2) (5) (9) (10) | AC-6 (1) (2) (3) (5) (7) (8) (9) (10) |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | AC-7 | AC-7 (2) |
| AC-8 | System Use Notification | AC-8 | AC-8 | AC-8 |
| AC-10 | Concurrent Session Control | Not Selected | AC-10 | AC-10 |
| AC-11 | Session Lock | Not Selected | AC-11 (1) | AC-11 (1) |
| AC-12 | Session Termination | Not Selected | AC-12 | AC-12 (1) |
| AC-14 | Permitted Actions Without Identification or Authentication | AC-14 | AC-14 | AC-14 |
| AC-17 | Remote Access | AC-17 | AC-17 (1) (2) (3) (4) (9) | AC-17 (1) (2) (3) (4) (9) |
| AC-18 | Wireless Access | AC-18 | AC-18 (1) | AC-18 (1) (3) (4) (5) |
| AC-19 | Access Control for Mobile Devices | AC-19 | AC-19 (5) | AC-19 (5) |
| AC-20 | Use of External Information Systems | AC-20 | AC-20 (1) (2) | AC-20 (1) (2) |
| AC-21 | Information Sharing | Not Selected | AC-21 | AC-21 |
| AC-22 | Publicly Accessible Content | AC-22 | AC-22 | AC-22 |
| AT | Awareness and Training | | | |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | AT-1 | AT-1 |
| AT-2 | Security Awareness Training | AT-2 | AT-2 (2) | AT-2 (2) |
| AT-3 | Role-Based Security Training | AT-3 | AT-3 | AT-3 (3) (4) |
| AT-4 | Security Training Records | AT-4 | AT-4 | AT-4 |
| AU | Audit and Accountability | | | |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | AU-1 | AU-1 |
| AU-2 | Audit Events | AU-2 | AU-2 (3) | AU-2 (3) |
| AU-3 | Content of Audit Records | AU-3 | AU-3 (1) | AU-3 (1) (2) |
| AU-4 | Audit Storage Capacity | AU-4 | AU-4 | AU-4 |
| AU-5 | Response to Audit Processing Failures | AU-5 | AU-5 | AU-5 (1) (2) |
| AU-6 | Audit Review, Analysis and Reporting | AU-6 | AU-6 (1) (3) | AU-6 (1) (3) (4) (5) (6) (7) (10) |
| AU-7 | Audit Reduction and Report Generation | Not Selected | AU-7 (1) | AU-7 (1) |
| AU-8 | Time Stamps | AU-8 | AU-8 (1) | AU-8 (1) |
| AU-9 | Protection of Audit Information | AU-9 | AU-9 (2) (4) | AU-9 (2) (3) (4) |
| AU-10 | Non-repudiation | Not Selected | Not Selected | AU-10 |
| AU-11 | Audit Record Retention | AU-11 | AU-11 | AU-11 |
| AU-12 | Audit Generation | AU-12 | AU-12 | AU-12 (1) (3) |
| CA | Security Assessment and Authorization | | | |
| CA-1 | Security Assessment and Authorization Policies and Procedures | CA-1 | CA-1 | CA-1 |
| CA-2 | Security Assessments | CA-2 (1) | CA-2 (1) (2) (3) | CA-2 (1) (2) (3) |
| CA-3 | System Interconnections | CA-3 | CA-3 (3) (5) | CA-3 (3) (5) |
| CA-5 | Plan of Action and Milestones | CA-5 | CA-5 | CA-5 |
| CA-6 | Security Authorization | CA-6 | CA-6 | CA-6 |
| CA-7 | Continuous Monitoring | CA-7 | CA-7 (1) | CA-7 (1) (3) |
| CA-8 | Penetration Testing | Not Selected | CA-8 (1) | CA-8 (1) |
| CA-9 | Internal System Connections | CA-9 | CA-9 | CA-9 |
| CM | Configuration Management | | | |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | CM-1 | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | CM-2 (1) (2) (3) (7) | CM-2 (1) (2) (3) (7) |
| CM-3 | Configuration Change Control | Not Selected | CM-3 (2) | CM-3 (1) (2) (4) (6) |
| CM-4 | Security Impact Analysis | CM-4 | CM-4 | CM-4 (1) |
| CM-5 | Access Restrictions for Change | Not Selected | CM-5 (1) (3) (5) | CM-5 (1) (2) (3) (5) |
| CM-6 | Configuration Settings | CM-6 | CM-6 (1) | CM-6 (1) (2) |
| CM-7 | Least Functionality | CM-7 | CM-7 (1) (2) (5)\* | CM-7 (1) (2) (5) |
| CM-8 | Information System Component Inventory | CM-8 | CM-8 (1) (3) (5) | CM-8 (1) (2) (3) (4) (5) |
| CM-9 | Configuration Management Plan | Not Selected | CM-9 | CM-9 |
| CM-10 | Software Usage Restrictions | CM-10 | CM-10 (1) | CM-10 (1) |
| CM-11 | User-Installed Software | CM-11 | CM-11 | CM-11 (1) |
| \*Company does not include CM-7 (4) in the Moderate Baseline. NIST supplemental guidance states that CM-7 (4) is not required if (5) is implemented. | | | | |
| CP | Contingency Planning | | | |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | CP-1 | CP-1 |
| CP-2 | Contingency Plan | CP-2 | CP-2 (1) (2) (3) (8) | CP-2 (1) (2) (3) (4) (5) (8) |
| CP-3 | Contingency Training | CP-3 | CP-3 | CP-3 (1) |
| CP-4 | Contingency Plan Testing | CP-4 | CP-4 (1) | CP-4 (1) (2) |
| CP-6 | Alternate Storage Site | Not Selected | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| CP-7 | Alternate Processing Site | Not Selected | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) |
| CP-8 | Telecommunications Services | Not Selected | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| CP-9 | Information System Backup | CP-9 | CP-9 (1) (3) | CP-9 (1) (2) (3) (5) |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | CP-10 (2) | CP-10 (2) (4) |
| IA | Identification and Authentication | | | |
| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1) (12) | IA-2 (1) (2) (3) (5) (8) (11) (12) | IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12) |
| IA-3 | Device Identification and Authentication | Not Selected | IA-3 | IA-3 |
| IA-4 | Identifier Management | IA-4 | IA-4 (4) | IA-4 (4) |
| IA-5 | Authenticator Management | IA-5 (1) (11) | IA-5 (1) (2) (3) (4) (6) (7) (11) | IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13) |
| IA-6 | Authenticator Feedback | IA-6 | IA-6 | IA-6 |
| IA-7 | Cryptographic Module Authentication | IA-7 | IA-7 | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) |
| IR | Incident Response | | | |
| IR-1 | Incident Response Policy and Procedures | IR-1 | IR-1 | IR-1 |
| IR-2 | Incident Response Training | IR-2 | IR-2 | IR-2 (1) (2) |
| IR-3 | Incident Response Testing | Not Selected | IR-3 (2) | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | IR-4 (1) | IR-4 (1) (2) (3) (4) (6) (8) |
| IR-5 | Incident Monitoring | IR-5 | IR-5 | IR-5 (1) |
| IR-6 | Incident Reporting | IR-6 | IR-6 (1) | IR-6 (1) |
| IR-7 | Incident Response Assistance | IR-7 | IR-7 (1) (2) | IR-7 (1) (2) |
| IR-8 | Incident Response Plan | IR-8 | IR-8 | IR-8 |
| IR-9 | Information Spillage Response | Not Selected | IR-9 (1) (2) (3) (4) | IR-9 (1) (2) (3) (4) |
| MA | Maintenance | | | |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | MA-1 | MA-1 |
| MA-2 | Controlled Maintenance | MA-2 | MA-2 | MA-2 (2) |
| MA-3 | Maintenance Tools | Not Selected | MA-3 (1) (2) (3) | MA-3 (1) (2) (3) |
| MA-4 | Nonlocal Maintenance | MA-4 | MA-4 (2) | MA-4 (2) (3) (6) |
| MA-5 | Maintenance Personnel | MA-5 | MA-5 (1) | MA-5 (1) |
| MA-6 | Timely Maintenance | Not Selected | MA-6 | MA-6 |
| MP | Media Protection | | | |
| MP-1 | Media Protection Policy and Procedures | MP-1 | MP-1 | MP-1 |
| MP-2 | Media Access | MP-2 | MP-2 | MP-2 |
| MP-3 | Media Marking | Not Selected | MP-3 | MP-3 |
| MP-4 | Media Storage | Not Selected | MP-4 | MP-4 |
| MP-5 | Media Transport | Not Selected | MP-5 (4) | MP-5 (4) |
| MP-6 | Media Sanitization | MP-6 | MP-6 (2) | MP-6 (1) (2) (3) |
| MP-7 | Media Use | MP-7 | MP-7 (1) | MP-7 (1) |
| PE | Physical and Environmental Protection | | | |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | PE-1 | PE-1 |
| PE-2 | Physical Access Authorizations | PE-2 | PE-2 | PE-2 |
| PE-3 | Physical Access Control | PE-3 | PE-3 | PE-3 (1) |
| PE-4 | Access Control for Transmission Medium | Not Selected | PE-4 | PE-4 |
| PE-5 | Access Control for Output Devices | Not Selected | PE-5 | PE-5 |
| PE-6 | Monitoring Physical Access | PE-6 | PE-6 (1) | PE-6 (1) (4) |
| PE-8 | Visitor Access Records | PE-8 | PE-8 | PE-8 (1) |
| PE-9 | Power Equipment and Cabling | Not Selected | PE-9 | PE-9 |
| PE-10 | Emergency Shutoff | Not Selected | PE-10 | PE-10 |
| PE-11 | Emergency Power | Not Selected | PE-11 | PE-11 (1) |
| PE-12 | Emergency Lighting | PE-12 | PE-12 | PE-12 |
| PE-13 | Fire Protection | PE-13 | PE-13 (2) (3) | PE-13 (1) (2) (3) |
| PE-14 | Temperature and Humidity Controls | PE-14 | PE-14 (2) | PE-14 (2) |
| PE-15 | Water Damage Protection | PE-15 | PE-15 | PE-15 (1) |
| PE-16 | Delivery and Removal | PE-16 | PE-16 | PE-16 |
| PE-17 | Alternate Work Site | Not Selected | PE-17 | PE-17 |
| PE-18 | Location of Information System Components | Not Selected | Not Selected | PE-18 |
| PL | Planning | | | |
| PL-1 | Security Planning Policy and Procedures | PL-1 | PL-1 | PL-1 |
| PL-2 | System Security Plan | PL-2 | PL-2 (3) | PL-2 (3) |
| PL-4 | Rules of Behavior | PL-4 | PL-4 (1) | PL-4 (1) |
| PL-8 | Information Security Architecture | Not Selected | PL-8 | PL-8 |
| PS | Personnel Security | | | |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | PS-1 | PS-1 |
| PS-2 | Position Risk Designation | PS-2 | PS-2 | PS-2 |
| PS-3 | Personnel Screening | PS-3 | PS-3 (3) | PS-3 (3) |
| PS-4 | Personnel Termination | PS-4 | PS-4 | PS-4 (2) |
| PS-5 | Personnel Transfer | PS-5 | PS-5 | PS-5 |
| PS-6 | Access Agreements | PS-6 | PS-6 | PS-6 |
| PS-7 | Third-Party Personnel Security | PS-7 | PS-7 | PS-7 |
| PS-8 | Personnel Sanctions | PS-8 | PS-8 | PS-8 |
| RA | Risk Assessment | | | |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | RA-1 | RA-1 |
| RA-2 | Security Categorization | RA-2 | RA-2 | RA-2 |
| RA-3 | Risk Assessment | RA-3 | RA-3 | RA-3 |
| RA-5 | Vulnerability Scanning | RA-5 | RA-5 (1) (2) (3) (5) (6) (8) | RA-5 (1) (2) (3) (4) (5) (6) (8) (10) |
| SA | System and Services Acquisition | | | |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | SA-1 | SA-1 |
| SA-2 | Allocation of Resources | SA-2 | SA-2 | SA-2 |
| SA-3 | System Development Life Cycle | SA-3 | SA-3 | SA-3 |
| SA-4 | Acquisition Process | SA-4 (10) | SA-4 (1) (2) (8) (9) (10) | SA-4 (1) (2) (8) (9) (10) |
| SA-5 | Information System Documentation | SA-5 | SA-5 | SA-5 |
| SA-8 | Security Engineering Principles | Not Selected | SA-8 | SA-8 |
| SA-9 | External Information System Services | SA-9 | SA-9 (1) (2) (4) (5) | SA-9 (1) (2) (4) (5) |
| SA-10 | Developer Configuration Management | Not Selected | SA-10 (1) | SA-10 (1) |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | SA-11 (1) (2) (8) | SA-11 (1) (2) (8) |
| SA-12 | Supply Chain Protection | Not Selected | Not Selected | SA-12 |
| SA-15 | Development Process, Standards and Tools | Not Selected | Not Selected | SA-15 |
| SA-16 | Developer-Provided Training | Not Selected | Not Selected | SA-16 |
| SA-17 | Developer Security Architecture and Design | Not Selected | Not Selected | SA-17 |
| SC | System and Communications Protection | | | |
| SC-1 | System and Communications Protection Policy and Procedures | SC-1 | SC-1 | SC-1 |
| SC-2 | Application Partitioning | Not Selected | SC-2 | SC-2 |
| SC-3 | Security Function Isolation | Not Selected | Not Selected | SC-3 |
| SC-4 | Information in Shared Resources | Not Selected | SC-4 | SC-4 |
| SC-5 | Denial of Service Protection | SC-5 | SC-5 | SC-5 |
| SC-6 | Resource Availability | Not Selected | SC-6 | SC-6 |
| SC-7 | Boundary Protection | SC-7 | SC-7 (3) (4) (5) (7) (8) (12) (13) (18) | SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21) |
| SC-8 | Transmission Confidentiality and Integrity | Not Selected | SC-8 (1) | SC-8 (1) |
| SC-10 | Network Disconnect | Not Selected | SC-10 | SC-10 |
| SC-12 | Cryptographic Key Establishment and Management | SC-12 | SC-12 (2) (3) | SC-12 (1) (2) (3) |
| SC-13 | Cryptographic Protection | SC-13 | SC-13 | SC-13 |
| SC-15 | Collaborative Computing Devices | SC-15 | SC-15 | SC-15 |
| SC-17 | Public Key Infrastructure Certificates | Not Selected | SC-17 | SC-17 |
| SC-18 | Mobile Code | Not Selected | SC-18 | SC-18 |
| SC-19 | Voice Over Internet Protocol | Not Selected | SC-19 | SC-19 |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) | SC-20 | SC-20 | SC-20 |
| SC-21 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | SC-21 | SC-21 | SC-21 |
| SC-22 | Architecture and Provisioning for Name / Address Resolution Service | SC-22 | SC-22 | SC-22 |
| SC-23 | Session Authenticity | Not Selected | SC-23 | SC-23 (1) |
| SC-24 | Fail in Known State | Not Selected | Not Selected | SC-24 |
| SC-28 | Protection of Information at Rest | Not Selected | SC-28 (1) | SC-28 (1) |
| SC-39 | Process Isolation | SC-39 | SC-39 | SC-39 |
| SI | System and Information Integrity | | | |
| SI-1 | System and Information Integrity Policy and Procedures | SI-1 | SI-1 | SI-1 |
| SI-2 | Flaw Remediation | SI-2 | SI-2 (2) (3) | SI-2 (1) (2) (3) |
| SI-3 | Malicious Code Protection | SI-3 | SI-3 (1) (2) (7) | SI-3 (1) (2) (7) |
| SI-4 | Information System Monitoring | SI-4 | SI-4 (1) (2) (4) (5) (14) (16) (23) | SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24) |
| SI-5 | Security Alerts, Advisories and Directives | SI-5 | SI-5 | SI-5 (1) |
| SI-6 | Security Function Verification | Not Selected | SI-6 | SI-6 |
| SI-7 | Software, Firmware and Information Integrity | Not Selected | SI-7 (1) (7) | SI-7 (1) (2) (5) (7) (14) |
| SI-8 | Spam Protection | Not Selected | SI-8 (1) (2) | SI-8 (1) (2) |
| SI-10 | Information Input Validation | Not Selected | SI-10 | SI-10 |
| SI-11 | Error Handling | Not Selected | SI-11 | SI-11 |
| SI-12 | Information Handling and Retention | SI-12 | SI-12 | SI-12 |
| SI-16 | Memory Protection | SI-16 | SI-16 | SI-16 |

The definitions in Table 13‑2. Control Origination and Definitions indicate where each security control originates.

Table 13‑2. Control Origination and Definitions

| Control Origination | Definition | Example |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the SP Name 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 system at the SP Name 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 system at the SP Name. | There are scans of the corporate network infrastructure; scans of databases and web-based application are system specific. |
| Configured by Customer | A control where the 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 the customer needs to provide additional hardware or software to meet the control requirement. | The customer provides a SAML SSO solution to implement two-factor authentication. |
| Shared | A control that is managed and implemented partially by the SP Name and partially by the customer. | Security awareness training must be conducted by both the SPN and the customer. |
| Inherited from pre-existing Company Authorization | A control that is inherited from another SP Name system that has already received a Company Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

\*Hyper Text Transport Protocol (http)

Responsible Role indicates the role of SP employee who can best respond to questions about the control that is described.

## Access Control (AC)

### AC-1 Access Control Policy and Procedures Requirements (L) (M)

The organization:

1. Develops, documents and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Reviews and updates the current:
   1. Access control policy [Company Assignment: at least every 3 years]; and
   2. Access control procedures [Company Assignment: at least annually].

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-1(a): | |
| Parameter AC-1(b)(1): | |
| Parameter AC-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b1 |  |
| Part b2 |  |

### AC-2 Account Management (L) (M)

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
7. Monitors the use of information system accounts;
8. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;
9. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;
10. Reviews accounts for compliance with account management requirements [Company Assignment: at least annually]; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(a): | |
| Parameter AC-2(e): | |
| Parameter AC-2(f): | |
| Parameter AC-2(j): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |
| Part h |  |
| Part i |  |
| Part j |  |
| Part k |  |

### AC-3 Access Enforcement (L) (M) (H)

The information system enforces 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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| AC-3 What is the solution and how is it implemented? |
| --- |
|  |

### AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

1. Enforces a limit of [Company Assignment: not more than three (3)] consecutive invalid logon attempts by a user during a [Company Assignment: fifteen (15) minutes]; and
2. Automatically [Selection: locks the account/node for a [Company Assignment: thirty (30) minutes]; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-7(a)-1: | |
| Parameter AC-7(a)-2: | |
| Parameter AC-7(b)-1: | |
| Parameter AC-7(b)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AC-8 System Use Notification (L) (M) (H)

The information system:

1. Displays to users [Assignment: organization-defined system use notification message or banner (Company Assignment: see additional Requirements and Guidance)] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
   1. Displays system use information [Assignment: organization-defined conditions (Company Assignment: see additional Requirements and Guidance)], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

AC-8 Additional Company Requirements and Guidance:

Requirement: The service provider shall determine elements of the environment that require the System Use Notification control. The elements of the environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-8(a): | |
| Parameter AC-8(c)-1: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Additional Company Requirements and Guidance

Requirement 1: The service provider shall determine elements of the environment that require the System Use Notification control. The elements of the environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement 2: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement 3: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 |  |
| Req. 2 |  |
| Req. 3 |  |

### AC-14 Permitted Actions without Identification or Authentication (L) (M) (H)

The organization:

1. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-14(a): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AC-17 Remote Access (L) (M) (H)

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information 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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AC-18 Wireless Access Restrictions (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AC-19 Access Control for Portable and Mobile Systems (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AC-20 Use of External Information Systems (L) (M) (H)

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AC-22 Publicly Accessible Content (L) (M) (H)

The organization:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [Company Assignment: at least quarterly] and removes such information, if discovered.

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-22: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

## Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Reviews and updates the current:
   1. Security awareness and training policy [Company Assignment: at least every 3 years]; and
   2. Security awareness and training procedures [Company Assignment: at least annually].

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AT-1(a): | |
| Parameter AT-1(b)(1): | |
| Parameter AT-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AT-2 Security Awareness (L) (M) (H)

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. [Company Assignment: at least annually] thereafter.

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AT-2(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### AT-3 Role-Based Security Training (L) (M) (H)

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. [Company Assignment: at least annually] thereafter.

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AT-3(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

#### AT-4 Security Training Records (L) (M)

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [Company Assignment: at least one year].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AT-4(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current:
   1. Audit and accountability policy [Company Assignment: at every 3 years]; and
   2. Audit and accountability procedures [Company Assignment: at least annually].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-1(a): | |
| Parameter AU-1(b)(1): | |
| Parameter AU-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AU-2 Audit Events (L) (M) (H)

The organization:

1. Determines that the information system is capable of auditing the following events: [Company Assignment: [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];
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [Company Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event].

AU-2 Additional Company Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

| AU-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-2(a): | |
| Parameter AU-2(d): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### AU-3 Content of Audit Records (L) (M) (H)

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects 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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-3 What is the solution and how is it implemented? |
| --- |
|  |

### AU-4 Audit Storage Capacity (L) (M) (H)

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

| AU-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-4: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-4 What is the solution and how is it implemented? |
| --- |
|  |

### AU-5 Response to Audit Processing Failures (L) (M) (H)

The information system:

1. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and
2. Takes the following additional actions: [Company Assignment: organization-defined actions to be taken; (overwrite oldest record)].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-5(a): | |
| Parameter AU-5(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AU-6 Audit Review, Analysis, and Reporting (L) (M) (H)

The organization:

1. Reviews and analyzes information system audit records [Company Assignment: at least weekly] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
2. Reports findings to [Assignment: organization-defined personnel or roles].

AU-6 Additional Company Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the Authorizing Official. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

| AU-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-6(a)-1: | |
| Parameter AU-6(a)-2: | |
| Parameter AU-6(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AU-8 Time Stamps (L) (M) (H)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: one second granularity of time measurement].

| AU-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-8(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### AU-9 Protection of Audit Information (L) (M) (H)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-9 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 What is the solution and how is it implemented? |
| --- |
|  |

### AU-11 Audit Record Retention (L) (M)

The organization retains audit records for [Company Assignment: at least ninety (90) days] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional Company Requirements and Guidance:

Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-11: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-11 What is the solution and how is it implemented? |
| --- |
|  |

### AU-12 Audit Generation (L) (M) (H)

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Company Assignment: all information system components where audit capability is deployed/available];
2. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-12(a): | |
| Parameter AU-12(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## Security Assessment and Authorization (CA)

### CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy [Company Assignment: at least every three (3) years]; and
   2. Security assessment and authorization procedures [Company Assignment: at least annually].

| CA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-1(a): | |
| Parameter CA-1(b)(1): | |
| Parameter CA-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### CA-2 Security Assessments (L) (M) (H)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [Company Assignment: at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [Company Assignment: individuals or roles to include the Company Program Management Office (PMO)].

CA-2 Additional Company Requirements and Guidance

Guidance: See the Company Documents page under Key Service

Provider (SP) Documents> Annual Assessment Guidance

https://www.company.gov/documents/

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-2(b): | |
| Parameter CA-2(d): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. Date of Authorization, | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

#### CA-2 (1) Control Enhancement (L) (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.

CA-2 (1) Additional Company Requirements and Guidance:

Requirement: For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO).

| CA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-2(1): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
|  |

### CA-3 System Interconnections (L)

The organization:

1. Authorizes connections from the information system to other information systems using Interconnection Security Agreements.
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements

Table 13‑3. CA-3 Authorized Connections

| Authorized Connections Information System Name | Name of Organization SP Name System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-3(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | See § 11 for information about implementation. |
| Part b | See Table 13‑2. Control Origination and Definitions and Table 11‑1. System Interconnections for information about implementation. |
| Part c |  |

### **CA-5 Plan of Action and Milestones (L)**

The organization:

1. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones [Company Assignment: at least monthly] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-5 Additional Company Requirements and Guidance:

Requirement: Plan of Action & Milestones (POA&M) must be provided at least monthly.

Guidance: See the Company Documents page under Key Service

Provider (SP) Documents> Plan of Action and Milestones (POA&M) Template Completion Guide

[https://www.company.gov/documents/](https://www.fedramp.gov/documents/)

| CA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-5(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### CA-6 Security Authorization (L) (M) (H)

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [Company Assignment: in accordance with OMB A-130 requirements or when a significant change occurs].

CA-6c Additional Company Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F ([SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)). 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: | |
| Parameter CA-6(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### CA-7 Continuous Monitoring (L) (M) (H)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [Assignment: organization-defined metrics] to be monitored;
2. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [Company Assignment: to meet Federal and Company requirements] [Assignment: organization-defined frequency].

CA-7 Additional Company Requirements and Guidance:

Requirement: Operating System Scans: at least monthly. Database and Web Application Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

Guidance: SPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

Guidance: See the Company Documents page under Key Service

Provider (SP) Documents> Continuous Monitoring Strategy Guide

[https://www.Company.gov/documents/](https://www.FedRAMP.gov/documents/)

| CA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-7(a): | |
| Parameter CA-7(b)-1: | |
| Parameter CA-7(b)-2: | |
| Parameter CA-7(g)-1: | |
| Parameter CA-7(g)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

CA-7 Additional Company Requirements and Guidance:

Requirement 1: Operating System Scans: at least monthly

Requirement 2: Database and Web Application Scans: at least monthly

Requirement 3: All scans performed by Independent Assessor: at least annually

| CA-7 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 |  |
| Req. 2 |  |
| Req. 3 |  |

### CA-9 Internal System Connections (L) (M) (H)

The organization:

1. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-9(a): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

## Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
2. Reviews and updates the current:
   1. Configuration management policy [Company Assignment: at least every three (3) years]; and
   2. Configuration management procedures [Company Assignment: at least annually].

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-1(a): | |
| Parameter CM-1(b)(1): | |
| Parameter CM-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CM-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### CM-2 Baseline Configuration (L) (M) (H)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

| CM-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 What is the solution and how is it implemented? |
| --- |
|  |

### CM-4 Security Impact Analysis (L) (M) (H)

The organization analyzes changes to the information system to determine potential security 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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CM-4 What is the solution and how is it implemented? |
| --- |
|  |

### CM-6 Configuration Settings (L) (M) (H)

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [Company Assignment: see CM-6(a) Additional Company Requirements and Guidance] that reflect the most restrictive mode consistent with operational requirements;

CM-6(a) Additional Company Requirements and Guidance:

Requirement 1: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. If no recognized USGCB is available for the technology in use, the SP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (<http://scap.nist.gov/>) validated or SCAP compatible (if validated checklists are not available).

Guidance: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>.

1. Implements the configuration settings;
2. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
3. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-6(a)-1: | |
| Parameter CM-6(a)-2: | |
| Parameter CM-6(c)-1: | |
| Parameter CM-6(c)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### CM-7 Least Functionality (L) (M) (H)

The organization:

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services [Company Assignment: United States Government Configuration Baseline (USGCB)]

CM-7 Additional Company Requirements and Guidance:

Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. If no recognized USGCB is available for the technology in use, the SP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Guidance: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>

Partially derived from AC-17 (8).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-7(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. Date of Authorization, | |

| CM-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### CM-8 Information System Component Inventory (L) (M) (H)

The organization:

1. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
2. Reviews and updates the information system component inventory [Company Assignment: at least monthly].

CM-8 Additional Company Requirements and Guidance:

Requirement: Must be provided at least monthly or when there is a change.

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-8(a)(4): | |
| Parameter CM-8(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### CM-10 Software Usage Restrictions (L) (M) (H)

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

| CM-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### CM-11 User-Installed Software (L) (M) (H)

The organization:

1. Establishes [Assignment: organization-defined policies] governing the installation of software by users;
2. Enforces software installation policies through [Assignment: organization-defined methods]; and
3. Monitors policy compliance [Company Assignment: Continuously (via CM-7 (5))].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-11(a): | |
| Parameter CM-11(b): | |
| Parameter CM-11(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
2. Reviews and updates the current:
   1. Contingency planning policy [Company Assignment: at least every three (3) years].; and
   2. Contingency planning procedures [Company Assignment: at least annually].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-1(a): | |
| Parameter CP-1(b)(1): | |
| Parameter CP-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system [Company Assignment: at least annually];
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
7. Protects the contingency plan from unauthorized disclosure and modification.

CP-2 Additional Company Requirements and Guidance:

Requirement: For JAB authorizations the contingency lists include designated Company personnel.

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-2(a)(6): | |
| Parameter CP-2(b): | |
| Parameter CP-2(d): | |
| Parameter CP-2(f): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

### CP-3 Contingency Training (L) (M) (H)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [Company Assignment: ten (10) days] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [Company Assignment: at least annually] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-3(a): | |
| Parameter CP-3(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CP-3 What is the solution and how is it implemented? |
| --- |
|  |

### CP-4 Contingency Plan Testing (L)

The organization:

1. Tests the contingency plan for the information system [Company Assignment: at least every three (3) years] using [Company Assignment: classroom exercises/table top written tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

CP-4(a) Additional Company Requirements and Guidance:

Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to Company prior to initiating testing. Test plans are approved and accepted by the JAB/AO prior to initiating testing.

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-4(a)-1: | |
| Parameter CP-4(a)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### CP-9 Information System Backup (L) (M) (H)

The organization:

CP-9 Additional Company Requirements and Guidance:

Requirement: The service provider shall determine what elements of the 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.

1. Conducts backups of user-level information contained in the information system [Company Assignment: daily incremental; weekly full]

CP-9 (a) Additional Company Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online).

1. Conducts backups of system-level information contained in the information system [Company Assignment: daily incremental; weekly full];

CP-9 (b) Additional Company Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online).

1. Conducts backups of information system documentation including security-related documentation [Company Assignment: daily incremental; weekly full ]; and

CP-9 (c) Additional Company Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online).

1. Protects the confidentiality, integrity, and availability of backup information at storage locations.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-9(a): | |
| Parameter CP-9(b): | |
| Parameter CP-9(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### CP-10 Information System Recovery and Reconstitution (L) (M) (H)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

| CP-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| CP-10 What is the solution and how is it implemented? |
| --- |
|  |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
2. Reviews and updates the current:
   1. Identification and authentication policy [Company Assignment: at least every three (3) years]; and
   2. Identification and authentication procedures [Company Assignment: at least annually].

| IA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-1(a): | |
| Parameter IA-1(a): | |
| Parameter IA-1(b)(1): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### IA-2 User Identification and Authentication (L) (M) (H)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

| IA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 What is the solution and how is it implemented? |
| --- |
|  |

#### IA-2 (1) Control Enhancement (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
|  |

#### IA-2 (12) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

IA-2 (12) Additional Company Requirements and Guidance:

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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
|  |

### IA-4 Identifier Management (L) (M)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [Company Assignment: at least two (2) years]; and
5. Disabling the identifier after [Company Assignment: ninety days for user identifiers (see additional requirements and guidance)]

IA-4e Additional Company Requirements and Guidance:

Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD clouds, see DoD website for specific DoD requirements that go above and beyond Company http://iase.disa.mil/cloud\_security/Pages/index.aspx.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-4(a): | |
| Parameter IA-4(d): | |
| Parameter IA-4(e): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

### IA-5 Authenticator Management (L) (M)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

**IA-5 Additional Company Requirements and Guidance:**

**Requirement:** Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 1. Link <https://pages.nist.gov/800-63-3>.

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(g): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |
| Part h |  |
| Part i |  |
| Part j |  |

#### IA-5 (1) Control Enhancement (L) (M)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
2. Enforces at least the following number of changed characters when new passwords are created: [Company Assignment: at least one (1)];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization- defined numbers for lifetime minimum, lifetime maximum];
5. Prohibits password reuse for [Company Assignment: twenty-four (24)] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

**IA-5 (1) a and d Additional Company Requirements and Guidance:**

**Guidance:** If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1) Guidance, the control may be considered compliant.

| IA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(1)(a): | |
| Parameter IA-5(1)(b): | |
| Parameter IA-5(1)(d): | |
| Parameter IA-5(1)(e): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

#### IA-5 (11) Control Enhancement (L) (M) (H)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

| IA-5 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(11): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (11) What is the solution and how is it implemented? |
| --- |
|  |

### IA-6 Authenticator Feedback (L) (M) (H)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-6 What is the solution and how is it implemented? |
| --- |
|  |

### IA-7 Cryptographic Module Authentication (L) (M) (H)

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

| IA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-7 What is the solution and how is it implemented? |
| --- |
|  |

### IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

| IA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 What is the solution and how is it implemented? |
| --- |
|  |

#### IA-8 (1) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) 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 | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (1) What is the solution and how is it implemented? |
| --- |
|  |

#### IA-8 (2) Control Enhancement (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
|  |

#### IA-8 (3) Control Enhancement (L) (M) (H)

The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

| IA-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-8(3): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
|  |

#### IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Company Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (4) What is the solution and how is it implemented? |
| --- |
|  |

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
2. Reviews and updates the current:
   1. Incident response policy [Company Assignment: at least every three (3) years]; and
   2. Incident response procedures [Company Assignment: at least annually].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IR-1(a): | |
| Parameter IR-1(b)(1): | |
| Parameter IR-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IR-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### IR-2 Incident Response Training (L) (M)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [Company Assignment: at least annually] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IR-2(a): | |
| Parameter IR-2(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### IR-4 Incident Handling (L) (M) (H)

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 Additional Company Requirements and Guidance:

Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

| IR-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| IR-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IR-5 What is the solution and how is it implemented? |
| --- |
|  |

### IR-6 Incident Reporting (L) (M) (H)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [Company Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)]; and
2. Reports security incident information to [Assignment: organization-defined authorities].

IR-6 Additional Company Requirements and Guidance

Requirement: Report security incident information according to Company Incident Communications Procedure.

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IR-6(a): | |
| Parameter IR-6(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### IR-7 Incident Response Assistance (L) (M) (H)

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

| IR-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 What is the solution and how is it implemented? |
| --- |
|  |

### IR-8 Incident Response Plan (L) (M) (H)

The organization:

1. Develops an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the incident response plan to [Company Assignment: see additional Company Requirements and Guidance].

IR-8(b) Additional Company Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated Company personnel.

1. Reviews the incident response plan [Company Assignment: at least annually];
2. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
3. Communicates incident response plan changes to [Company Assignment: see additional Company Requirements and Guidance].

IR-8(e) Additional Company Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated Company personnel.

1. Protects the incident response plan from unauthorized disclosure and modification.

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IR-8(a)(8): | |
| Parameter IR-8(b): | |
| Parameter IR-8(c): | |
| Parameter IR-8(e): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
2. Reviews and updates the current:
   1. System maintenance policy [Company Assignment: at least every three (3) years]; and
   2. System maintenance procedures [Company Assignment: at least annually].

| MA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MA-1(a): | |
| Parameter MA-1(b)(1): | |
| Parameter MA-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### MA-2 Controlled Maintenance (L) (M) (H)

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

| MA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MA-2(c): | |
| Parameter MA-2(f): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| MA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

### MA-4 Remote Maintenance (L) (M) (H)

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

| MA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| MA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

### MA-5 Maintenance Personnel (L) (M) (H)

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates 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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| MA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
3. Media protection policy [Company Assignment: at least every three (3) years]; and
4. Media protection procedures [Company Assignment: at least annually].

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MP-1(a): | |
| Parameter MP-1(b)(1): | |
| Parameter MP-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### MP-2 Media Access (L) (M)

The organization restricts 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: | |
| Parameter MP-2-1: | |
| Parameter MP-2-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| MP-2 What is the solution and how is it implemented? |
| --- |
|  |

### MP-6 Media Sanitization and Disposal (L) (M)

The organization:

1. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MP-6(a)-1: | |
| Parameter MP-6(a)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### MP-7 Media Use (L) (M) (H)

The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

| MP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MP-7-1: | |
| Parameter MP-7-2: | |
| Parameter MP-7-3: | |
| Parameter MP-7-4: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| MP-7 What is the solution and how is it implemented? |
| --- |
|  |

## Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy [Company Assignment: at least every three (3) years]; and
   2. Physical and environmental protection procedures [Company Assignment: at least annually].

| PE-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-1(a): | |
| Parameter PE-1(b)(1): | |
| Parameter PE-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PE-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### PE-2 Physical Access Authorizations (L) (M)

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [Company Assignment: at least annually]; and
4. Removes individuals from the facility access list when access is no longer required.

| PE-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-2(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### PE-3 Physical Access Control (L) (M) (H)

The organization:

1. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by:
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [Company Assignment: SP defined physical access control systems/devices AND guards];
2. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
3. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [Company Assignment: in all circumstances within restricted access area where the information system resides];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [Assignment: organization-defined physical access devices] every [Company Assignment: at least annually]; and
7. Changes combinations and keys [Company Assignment: at least annually] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| PE-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-3(a): | |
| Parameter PE-3(a)(2): | |
| Parameter PE-3(b): | |
| Parameter PE-3(c): | |
| Parameter PE-3(d): | |
| Parameter PE-3(f)-1: | |
| Parameter PE-3(f)-2: | |
| Parameter PE-3(g): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

### PE-6 Monitoring Physical Access (L) (M) (H)

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [Company Assignment: at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

| PE-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-6(b)-1: | |
| Parameter PE-6(b)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### PE-8 Visitor Access Records (L) (M) (H)

The organization:

1. Maintains visitor access records to the facility where the information system resides for [Company Assignment: for a minimum of one (1) year]; and
2. Reviews visitor access records [Company Assignment: at least monthly]

| PE-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-8(a): | |
| Parameter PE-8(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### PE-12 Emergency Lighting (L) (M) (H)

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

| PE-12 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-12 What is the solution and how is it implemented? |
| --- |
|  |

### PE-13 Fire Protection (L) (M) (H)

The organization employs and maintains fire suppression and detection devices/systems for the information system 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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-13 What is the solution and how is it implemented? |
| --- |
|  |

### PE-14 Temperature and Humidity Controls (L) (M) (H)

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [Company Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments]; and

PE-14 (a) Additional Company Requirements and Guidance:   
Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

1. Monitors temperature and humidity levels [Company Assignment: continuously].

| PE-14 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-14(a): | |
| Parameter PE-14(b): | |
| Parameter PE-14(b) Additional: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### PE-15 Water Damage Protection (L) (M) (H)

The organization protects the information 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 | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-15 What is the solution and how is it implemented? |
| --- |
|  |

### PE-16 Delivery and Removal (L) (M) (H)

The organization authorizes, monitors, and controls [Company Assignment: all information system components] entering and exiting the facility and maintains records of those items.

| PE-16 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-16: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PE-16 What is the solution and how is it implemented? |
| --- |
|  |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
2. Reviews and updates the current:
   1. Security planning policy [Company Assignment: at least every three (3) years]; and
   2. Security planning procedures [Company Assignment: at least annually].

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PL-1(a): | |
| Parameter PL-1(b)(1): | |
| Parameter PL-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PL-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### PL-2 System Security Plan (L) (M) (H)

The organization:

1. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
3. Reviews the security plan for the information system [Company Assignment: at least annually];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PL-2(b): | |
| Parameter PL-2(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

### PL-4 Rules of Behavior (L) (M)

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Reviews and updates the rules of behavior [Company Assignment: at least every three (3) years]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PL-4(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
   1. Personnel security policy [Company Assignment: at least every three (3) years]; and
   2. Personnel security procedures [Company Assignment: at least annually].

| PS-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-1(a): | |
| Parameter PS-1(b)(1): | |
| Parameter PS-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PS-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### PS-2 Position Categorization (L) (M)

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises position risk designations [Company Assignment: at least every three (3) years].

| PS-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-2(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PS-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### PS-3 Personnel Screening (L) (M) (H)

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [Company Assignment: 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: | |
| Parameter PS-3(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PS-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### PS-4 Personnel Termination (L) (M)

The organization, upon termination of individual employment:

1. Disables information system access within [Company Assignment: same day];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

| PS-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-4(a): | |
| Parameter PS-4(c): | |
| Parameter PS-4(f)-1: | |
| Parameter PS-4(f)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PS-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

### PS-5 Personnel Transfer (L) (M)

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [Assignment: organization-defined personnel or roles] within [Company Assignment: within five days of the formal transfer action (DoD 24 hours)].

| PS-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-5(b)-1: | |
| Parameter PS-5(b)-2: | |
| Parameter PS-5(d)-1: | |
| Parameter PS-5(d)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PS-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### PS-6 Access Agreements (L) (M)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [Company Assignment: at least annually]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Company Assignment: at least annually].

| PS-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-6(b): | |
| Parameter PS-6(c)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PS-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### PS-7 Third-Party Personnel Security (L) (M)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Company Assignment: same day]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-7(d)-1: | |
| Parameter PS-7(d)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PS-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

### PS-8 Personnel Sanctions (L) (M)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| PS-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-8(b)-1: | |
| Parameter PS-8(b)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| PS-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy [Company Assignment: at least every three (3) years]; and
   2. Risk assessment procedures [Company Assignment: at least annually].

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter RA-1(a): | |
| Parameter RA-1(b)(1): | |
| Parameter RA-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| RA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### RA-2 Security Categorization (L) (M) (H)

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

| RA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### RA-3 Risk Assessment (L) (M)

The organization:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
2. Documents risk assessment results in [Selection: security plan; risk assessment report; [Company Assignment: security assessment report]];
3. Reviews risk assessment results [Company Assignment: in accordance with OMB A-130 requirements or when a significant change occurs];
4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
5. Updates the risk assessment [Company Assignment: in accordance with OMB A-130 requirements or when a significant change occurs] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3 Additional Company Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F

RA-3 (d) Requirement: Include all Authorizing Officials; for JAB authorizations to include Company.

| RA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter RA-3(b): | |
| Parameter RA-3(c): | |
| Parameter RA-3(d): | |
| Parameter RA-3(e): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

### RA-5 Vulnerability Scanning (L) (M) (H)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [Company Assignment: monthly operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

RA-5 (a) Additional Company Requirements and Guidance:

Requirement: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

1. Employs vulnerability scanning tools and techniques that promote 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 and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [Company Assignment: 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; and
4. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

RA-5 (e) Additional Company Requirements and Guidance:

Requirement: To include all Authorizing Officials; for JAB authorizations to include Company.

RA-5 Additional Company Requirements and Guidance

Guidance: See the Company Documents page under Key Service

Provider (SP) Documents> Vulnerability Scanning Requirements

[https://www.Company.gov/documents/](https://www.FedRAMP.gov/documents/)

| RA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter RA-5(a): | |
| Parameter RA-5(d): | |
| Parameter RA-5(e): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [Company Assignment: at least every three (3) years]; and
   2. System and services acquisition procedures [Company Assignment: at least annually].

| SA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-1(a): | |
| Parameter SA-1(b)(1): | |
| Parameter SA-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### SA-2 Allocation of Resources (L) (M) (H)

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### SA-3 System Development Life Cycle (L) (M) (H)

The organization:

1. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-3(a): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

SA-4 Additional Company Requirements and Guidance:

Requirement: The service provider must comply 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).

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.   
See <https://www.niap-ccevs.org/Product/>

| SA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

### SA-5 Information System Documentation (L) (M)

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [Assignment: organization-defined personnel or roles)].

| SA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-5(c): | |
| Parameter SA-5(e): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

### SA-9 External Information System Services (L) (M) (H)

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [Company Assignment: Company Security Controls Baseline(s) if Federal information is processed or stored within the external system] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [Company Assignment: Federal/Company Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored] to monitor security control compliance by external service providers on an ongoing basis.

Additional Company Requirements and Guidance

Guidance: See the Company Documents page under Key Service Provider (SP) Documents> Continuous Monitoring Strategy Guide  
[https://www.Company.gov/documents](https://www.FedRAMP.gov/documents)

Guidance: Independent Assessors should assess the risk associated with the use of external services. See the Company page under Key Service Provider (SP) Documents>Company Authorization Boundary Guidance

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-9(a): | |
| Parameter SA-9(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. Date of Authorization | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy [Company Assignment: at least every three (3) years]; and
   2. System and communications protection procedures [Company Assignment: at least annually].

| SC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-1(a): | |
| Parameter SC-1(b)(1): | |
| Parameter SC-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### SC-5 Denial of Service Protection (L) (M) (H)

The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].

| SC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-5-1: | |
| Parameter SC-5-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-5 What is the solution and how is it implemented? |
| --- |
|  |

### SC-7 Boundary Protection (L) (M) (H)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

| SC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

### SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

SC-12 Additional Company Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

| SC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-12: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 What is the solution and how is it implemented? |
| --- |
|  |

### SC-13 Use of Cryptography (L) (M) (H)

The information system implements [Company Assignment: FIPS-validated or NSA-approved cryptography] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| SC-13 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-13: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-13 What is the solution and how is it implemented? |
| --- |
|  |

### SC-15 Collaborative Computing Devices (L) (M) (H)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions:[Company Assignment: no exceptions] and
2. Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional Company Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-15(a): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

SC-15 Additional Company Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 |  |

### SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

| SC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

| SC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-21 What is the solution and how is it implemented? |
| --- |
|  |

### SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| SC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-22 What is the solution and how is it implemented? |
| --- |
|  |

### SC-39 Process Isolation (L) (M) (H)

The information system maintains a separate execution domain for each executing process.

| SC-39 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SC-39 What is the solution and how is it implemented? |
| --- |
|  |

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
3. System and information integrity policy [Company Assignment: at least every three (3) years]; and
4. System and information integrity procedures [Company Assignment: at least at least annually].

| SI-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-1(a): | |
| Parameter SI-1(b)(1): | |
| Parameter SI-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SI-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

### SI-2 Flaw Remediation (L) (M) (H)

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [Company Assignment: thirty 30 days of release of updates] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-2(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### SI-3 Malicious Code Protection (L) (M)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [Company Assignment: at least weekly] and real-time scans of files from external sources at [Company Assignment: to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [Company Assignment: to include alerting administrator or defined security personnel] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-3(c)(1)-1: | |
| Parameter SI-3(c)(1)-2: | |
| Parameter SI-3(c)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### SI-4 Information System Monitoring (L) (M) (H)

The organization:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
3. Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SI-4 Additional Company Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

| SI-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-4(a)(1): | |
| Parameter SI-4(b): | |
| Parameter SI-4(g)-1: | |
| Parameter SI-4(g)-2: | |
| Parameter SI-4(g)-3: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

### SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

1. Receives information system security alerts, advisories, and directives from [Company Assignment: to include US-CERT] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [Company Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

| SI-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-5(a): | |
| Parameter SI-5(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. ,Date of Authorization | |

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

### SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

| SI-12 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of Authorization | |

| SI-12 What is the solution and how is it implemented? |
| --- |
|  |

### SI-16 Memory Protection (L) (M) (H)

The information system implements [Assignment: organization-defined fail-safe procedures] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-16-1: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Company Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| SI-16 What is the solution and how is it implemented? |
| --- |
|  |

# Acronyms

The master list of Company acronym and glossary definitions for all Company templates is available on the Company website [Documents](https://www.fedramp.gov/documents) page.

Please send suggestions about corrections, additions, or deletions to info@company.gov.

# Systems Security Plan Attachments

Instruction: Attach any documents that are referred to in the Information System Name (Enter Information System Abbreviation) System Security Plan. Documents and attachments should, provide the title, version and exact file name, including the file extension. All attachments and associated documents must be delivered separately. No embedded documents will be accepted.

Delete this and all other instructions from your final version of this document.

# Attachments

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

* The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15‑1. to differentiate between them using the “xx” portion of the File Name. Example Enter Information System Abbreviation A1 ISPP xx v1.0. Delete the “xx” if there is only one document.
* Enter the file extension for each attachment.
* Do not change the Version Number in the File Name in Table 15‑1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15‑1. Names of Provided Attachments

| Attachment | File Name | File Extension |
| --- | --- | --- |
| Information Security Policies and Procedures | Enter Information System Abbreviation A1 ISPP xx v1.0 | . enter extension |
| User Guide | Enter Information System Abbreviation A2 UG v1.0 | . enter extension |
| Digital Identity Worksheet | Included in Section 15 |  |
| PTA | Included in Section 15 |  |
| PIA If needed) | Enter Information System Abbreviation A4 PIA v1.0 | . enter extension |
| Rules of Behavior | Enter Information System Abbreviation A5 ROB v1.0 | . enter extension |
| Information System Contingency Plan | Enter Information System Abbreviation A6 ISCP v1.0 | . enter extension |
| Configuration Management Plan | Enter Information System Abbreviation A7 CMP v1.0 | . enter extension |
| Incident Response Plan | Enter Information System Abbreviation A8 IRP v1.0 | . enter extension |
| CIS Workbook | Enter Information System Abbreviation A9 CIS Workbook v1.0 | . enter extension |
| FIPS 199 | Included in Section 15 |  |
| Inventory | Enter Information System Abbreviation A13 INV v1.0 | . enter extension |

1. Information Security Policies and Procedures

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

1. User Guide

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality.

1. Digital Identity Worksheet

This Attachment Section has been revised to include the Digital Identity template. Therefore, a separate attachment is not needed. Delete this note and all other instructions from your final version of this document.

The Digital Identity section explains the objective for selecting the appropriate Digital Identity levels for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 3, Digital Identity Guidelines.

### Introduction and Purpose

This document provides guidance on digital identity services (Digital Identity, which is the process of establishing confidence in user identities electronically presented to an information system). Authentication focuses on the identity proofing process (IAL), the authentication process (AAL), and the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) (FAL). NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Level of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

NIST SP 800-63-3 can be found at the following URL: [NIST SP 800-63-3](https://pages.nist.gov/800-63-3/)

### Information System Name/Title

This Digital Identity Plan provides an overview of the security requirements for the Information System Name (Enter Information System Abbreviation) in accordance with NIST SP 800-63-3.

Table 15‑2. Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| Enter FedRAMP Application Number. | Information System Name | Enter Information System Abbreviation |

### Digital Identity Level Definitions

NIST SP 800-63-3 defines three levels in each of the components of identity assurance to categorize a federal information system’s Digital Identity posture. NIST SP 800-63-3 defines the Digital Identity levels as:

* IAL – refers to the identity proofing process.
* AAL – refers to the authentication process.
* FAL – refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

Company maps its system categorization levels to NIST 800-63-3’s levels as shown in Table 15-3:

Table 15‑3. Mapping Company Levels to NIST SP 800-63-3 Levels

| Company System Categorization | Identity Assurance Level (IAL) | Authenticator Assurance Level (AAL) | Federation Assurance Level (FAL) |
| --- | --- | --- | --- |
| **High** | IAL3: In-person, or supervised remote identity proofing | AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques | FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Moderate** | IAL2: In-person or remote, potentially involving a “trusted referee” | AAL2: Multi-factor required, using approved cryptographic techniques | FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Low** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor | FAL1: Assertion is digitally signed by the identity provider |
| **Company Tailored LI-SaaS** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor | FAL1: Assertion is digitally signed by the identity provider |

Selecting the appropriate Digital Identity level for a system enables the system owner to determine the right system authentication technology solution for the selected Digital Identity levels. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63-3.

### Review Maximum Potential Impact Levels

SP Name has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user’s asserted identity. SP Name has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 15‑4. Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 15‑4. Potential Impacts for Assurance Levels

|  | Assurance Level Impact Profile | | |
| --- | --- | --- | --- |
| Potential Impact Categories | 1 | 2 | 3 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | High |
| Financial loss or agency liability | Low | Mod | High |
| Harm to agency programs or public interests | N/A | Low/Mod | High |
| Unauthorized release of sensitive information | N/A | Low/Mod | High |
| Personal Safety | N/A | Low | Mod/High |
| Civil or criminal violations | N/A | Low/Mod | High |

### Digital Identity Level Selection

Instruction: Select the lowest level that will cover all potential impact identified from Table 15‑4. Potential Impacts for Assurance Levels.

Delete this instruction from your final version of this document.

The SP Name has identified that they support the Digital Identity Level that has been selected for the Information System Name as noted in Table 15‑5. Digital Identity Level. The selected Digital Identity Level indicated is supported for federal agency consumers of the Service offering. Implementation details of the Digital Identity mechanisms are provided in the System Security Plan under control IA-2.

Table 15‑5. Digital Identity Level

| Digital Identity Level | Maximum Impact Profile | Selection |
| --- | --- | --- |
| Level 1: AAL1, IAL1, FAL1 | Low |  |
| Level 2: AAL2, IAL2, FAL2 | Moderate |  |
| Level 3: AAL3, IAL3, FAL3 | High |  |

1. PTA / PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following Company website page: [Templates](https://www.fedramp.gov/templates).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in Attachment 12, Company Laws and Regulations.

### Privacy Overview and Point of Contact (POC)

The Table 15‑6. Information System Name Privacy POC individual is identified as the Information System Name Privacy Officer and POC for privacy at SP Name.

Table 15‑6. Information System Name Privacy POC

| Name | Click here to enter text. |
| --- | --- |
| Title | Click here to enter text. |
| SP / Organization | Click here to enter text. |
| Address | Click here to enter text. |
| Phone Number | Click here to enter text. |
| Email Address | Click here to enter text. |

#### Applicable Laws and Regulations

The Company Laws and Regulations may be found on: [Templates](https://www.fedramp.gov/templates). A summary of Company Laws and Regulations is included in the System Security Plan (SSP) Attachment 12, Company Laws and Regulations.

Table 12‑1. Information System Name Laws and Regulations include additional laws and regulations that are specific to Information System Name. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 15‑7. Information System Name Laws and Regulations

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### Applicable Standards and Guidance

The Company Standards and Guidance may be found on: [Templates](https://www.fedramp.gov/templates). The Company Standards and Guidance is included in the System Security Plan (SSP) ATTACHMENT 12 – Company Laws and Regulations. For more information, see the Company website.

Table 12‑2. Information System Name Standards and Guidance includes any additional standards and guidance that are specific to Information System Name. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table 15‑8. Information System Name Standards and Guidance

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### Personally Identifiable Information (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

* Social Security numbers
* Passport numbers
* Driver’s license numbers
* Biometric information
* DNA information
* Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

### Privacy Threshold Analysis

SP Name performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the Information System Name (Enter Information System Abbreviation) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by SP Name can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

|  |  |
| --- | --- |
| Select One | Does the ISA collect, maintain, or share PII in any identifiable form? |
| Select One | Does the ISA collect, maintain, or share PII information from or about the public? |
| Select One | Has a Privacy Impact Assessment ever been performed for the ISA? |
| Select One | Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  If yes; the SORN identifier and name is: Enter SORN ID/Name. |

If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.

#### Designation

Check one.

|  |  |
| --- | --- |
|  | A Privacy Sensitive System |
|  | Not a Privacy Sensitive System (in its current version) |

The Privacy Impact Assessment Template can be found on the following Company website page: [Templates](https://www.fedramp.gov/templates).

1. Rules of Behavior

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality.

The RoB describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a SP to implement rules of behavior.

The Rules of Behavior Template can be found on the following Company website page: [Templates](https://www.fedramp.gov/templates).

The Template provides two example sets of rules of behavior: one for Internal Users and one for External Users. The SP should modify each of these two sets to define the rules of behavior necessary to secure their system.

1. Information System Contingency Plan

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality.

The Information System Contingency Plan Template can be found on the following Company website page: [Templates](https://www.fedramp.gov/templates).

The Information System Contingency Plan Template is provided for SPs, 3PAOs, government contractors working on Company projects, government employees working on Company projects and any outside organizations that want to make use of the Company Contingency Planning process.

1. Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality.

1. Incident Response Plan

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

1. CIS Workbook

All Authorization Packages must include Control Implementation Summary (CIS) Workbook attachment, which will be reviewed for quality.

The Template can be found on the following Company website page: [Templates](https://www.fedramp.gov/templates).

1. FIPS 199

This Attachment Section has been revised to include the FIPS 199 Template. Therefore, a separate PTA attachment is not needed. Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality.

The FIPS-199 Categorization report includes the determination of the security impact level for the environment that may host any or all of the service models: IaaS, PaaS and SaaS. The ultimate goal of the security categorization is for the SP to be able to select and implement the Company security controls applicable to its environment.

### Introduction and Purpose

This section is intended to be used by service providers who are applying for an Authorization through the U.S. federal government Company program.

The Federal Information Processing Standard 199 (FIPS 199) Categorization (Security Categorization) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (Company) authorizing officials. The FIPS199 Categorization report includes the determination of the security impact level for the environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the Service provider (SP) to be able to select and implement the Company security controls applicable to its environment.

The purpose of the FIPS199 Categorization report is for the SP to assess and complete the categorization of their environment, to provide the categorization to the System Owner/Certifier and the Company Joint Authorization Board (JAB) and in helping them to make a determination of the SP’s ability to host systems at that level. The completed security categorization report will aid the SP in selection and implementation of Company security controls at the determined categorization level.

### Scope

The scope of the FIPS199 Categorization report includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume II Revision 1 Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

### System Description

The Information System Name system has been determined to have a security categorization of Choose level.

Instruction: Insert a brief high-level description of the system, the system environment and the purpose of the system. The description should be consistent with the description found in the System Security Plan (SSP).   
Delete this instruction from your final version of this document.

### Methodology

Instruction: The SP should review the NIST Special Publication 800-60 Volume 2 Revision 1 Appendix C Management and Support Information and Information System Impact Levels and Appendix D Impact Determination for Mission-Based Information and Information Systems to assess the recommended impact level for each of the information types. For more information, the SP should also consult Appendix D.2. After reviewing the NIST guidance on Information Types, the SP should fill out Table 15‑9. SP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1.   
Delete this instruction from your final version of this document.

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS PUB 199 is the high watermark for the impact level of all the applicable information types.

The FIPS PUB 199 analysis represents the information type and sensitivity levels of the SP’s Service offering (and is not intended to include sensitivity levels of agency data). Customer agencies will be expected to perform a separate FIPS 199 Categorization report analysis for their own data hosted on the SP’s environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

Instruction: In the first three columns, put the NIST SP-60 V2 R1 recommended impact level. In the next three columns, put in the SP determined recommended impact level. If the SP determined recommended impact level does not match the level recommended by NIST, put in an explanation in the last column as to why this decision was made.   
Delete this instruction from your final version of this document.

The Table 15‑9. SP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1below uses the NIST SP 800-60 V2 R1 Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table 15‑9. SP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

| Information Type | NIST SP 800-60 V2 R1  Recommended Confidentiality Impact Level | NIST SP 800-60 V2 R1  Recommended Integrity Impact Level | NIST SP 800-60 V2 R1  Recommended Availability Impact Level | SP Selected Confidentiality Impact Level | SP Selected Integrity Impact Level | SP Selected Availability Impact Level | Statement  for Impact Adjustment Justification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |

1. Separation of Duties Matrix

All Authorization Packages have the option to provide a Separation of Duties Matrix attachment, which will be reviewed for quality.

Attachment 11, Separation of Duties Matrix is referenced in the following control:

AC-5 Separation of Duties Additional Company Requirements and Guidance

1. Company Laws and Regulations

The Table 15‑10. Company Templates that Reference Company Laws and Regulations Standards and Guidance lists all of the Company templates in which Company laws, regulations, standards and guidance are referenced.

Table 15‑10. Company Templates that Reference Company Laws and Regulations Standards and Guidance

| Phase | | Document Title | |
| --- | --- | --- | --- |
| Document Phase | | SSP | System Security Plan |
|  | SSP Attachment 4 | PTA/PIA | Privacy Threshold Analysis and Privacy Impact Assessment |
|  | SSP Attachment 6 | ISCP | Information System Contingency Plan |
|  | SSP Attachment 10 | FIPS 199 | FIPS 199 Categorization |
| Assess Phase | | SAP | Security Assessment Plan |
| Authorize Phase | | SAR | Security Assessment Report |

The Company Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: [Templates](https://www.fedramp.gov/templates).

Note: All NIST Computer Security Publications can be found at the following  
URL: <http://csrc.nist.gov/publications/PubsSPs.html>

1. Company Inventory Workbook

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, Company will accept this inventory workbook as the inventory information required by the following:

* System Security Plan
* Security Assessment Plan
* Security Assessment Report
* Information System Contingency Plan
* Initial POAM
* Monthly Continuous Monitoring (POAM or as a separate document)

The Company Inventory Workbook can be found on the following Company website page: [Templates](https://www.fedramp.gov/templates).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.