FedRAMP® System Security Plan (SSP) Appendix A: High FedRAMP Security Controls

for <Insert CSP Name>

<Insert CSO Name>

<Insert Version X.X>

<Insert MM/DD/YYYY>

TEMPLATE REVISION HISTORY

Date	Version	Pages	Description	Author
06/30/2023	1.0	All	Initial publication. SSP security control sections are now provided as separate templates.	FedRAMP PMO
08/30/2023	1.1	All	Separate parameter fields were added for control sub-parts with multiple parameters. Minor editorial and formatting changes.	FedRAMP PMO
02/15/2024	1.2	All	Fixed typos	FedRAMP PMO

How to contact us

For questions about FedRAMP, or for questions about this document including how to use it, contact info@FedRAMP.gov.

For more information about FedRAMP, see www.FedRAMP.gov.

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

Appendix A High: <CSO> FedRAMP Security Controls

Below is the baseline template for the High impact security controls.

Instructions:

A cloud service provider (CSP) is encouraged to maintain the controls as a separate document from the System Security Plan (SSP) as the size will impact the level of effort needed to review/edit the SSP.

- *The controls tables describe the security controls as they are implemented for the system. For each control, it is important to describe **how** the control is implemented and **from where the control originates** so that it is clear whose responsibility it is to implement, manage, and monitor the control.*
- *Controls inheritance needs to be considered for each control – both from the perspective of a CSP inheriting controls from another CSP and inheritability of controls from a CSP to its customers (agencies or other CSPs). Please see the use case guidance, below:*
    - *For controls that are inherited from another CSP, the inheriting CSP should ensure that the "Inherited" box is selected with the name of the CSP being inherited from and that the control solution description states **what** functionality is being inherited from the other CSP.*
        - *Note that "-1" controls (AC-1, AU-1, SC-1, etc.) are **not** 100% inherited; the inheriting CSP must describe their functions to enable inheritance; in some cases, the role may be minimal.*
        - *Please remember that "inheritance" can be claimed from FedRAMP Authorized services only. If a system or service is not FedRAMP Authorized, a CSP is fully responsible for the control (though another entity may perform its function).*
    - *For controls defined as fully inheritable by the customer:*
        - *A CSP is responsible for ensuring its implementation meets federal/FedRAMP control requirements.*

- *A third-party assessment organization (3PAO) is required to validate that inherited security features can be inherited.*
- *For a control that can only be inherited, under a specific use case:*
  - *The CSP must describe that use case in the SSP.*
  - *The 3PAO is required to validate the control inheritability (as dictated by the use case).*
- *For controls defined as a customer responsibility, agencies are responsible for implementing, documenting, and testing the control.*
- *For shared responsibility controls:*
  - *Function(s), provided by a CSP, must be clearly documented in the SSP, specifying a CSP's responsibilities AND the responsibilities provided, or configured by, their agency customer.*
  - *A 3PAO is required to test a CSP's responsibilities.*
- *For all controls, if a CSP provides options for an agency/customer, in implementing a control, the CSP must make clear what options are compliant with federal policy.*
- *A CSP is NOT responsible for having their agency customer's implementation of inherited controls tested.*
- *A CSP is NOT responsible for having customer-responsible controls tested.*

- *Throughout the controls, policies and procedures must be explicitly referenced (title and date or version and the applicable section or paragraph numbers) so that it's clear which document is being referred to and where, within the document, applicable details can be found.*

Delete this instructional text from your final version of this document.

Instructions:

In the sections that follow, 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

CSP and by their customer. Use the definitions, in the table that follows, to indicate where each security control originates from. Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version and the applicable section or paragraph numbers) so that it is clear which document is being referred to. Section numbers, or similar mechanisms, should allow the reviewer to easily find the reference.

For SaaS and PaaS systems, that are inheriting controls from an IaaS (or anything lower in the stack), the "Inherited" check box must be checked, and the implementation description must simply say "Inherited." FedRAMP reviewers will determine whether the control-set is appropriate or not.

The NIST term "Organization Defined" must be interpreted as being a CSP's responsibility unless otherwise indicated. In some cases, the JAB has chosen to define or provide parameters, and in others, they have left the decision up to CSPs.

Please note: CSPs should not modify the control requirement text, including the parameter assignment instructions and additional FedRAMP requirements. CSP responses must be documented in the "Control Summary Information" and "What is the solution and how is it implemented?" tables.

Delete this instructional text from your final version of this document.

The definitions in Table A-1. Control Origination and Definitions indicate where each security control originates.

Table A-1. Control Origination and Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from a CSP's corporate network.	DNS, from the corporate network, provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular CSP system and the control is not part of the standard corporate controls.	A unique host-based intrusion detection system (HIDs) is available on the service offering platform but is not available on the corporate network.

Control Origination	Definition	Example
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls specific to a particular system.	There are scans of the corporate network infrastructure; scans of databases and web-based applications are system specific.
Configured by Customer	A control where 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 a CSP and partially by their customer.	Security awareness training must be conducted by both the CSPN and the customer.
Inherited from pre-existing FedRAMP Authorization	A control that is inherited from another CSP system that has already received a FedRAMP authorization.	A PaaS or SaaS provider inherits PE controls from an IaaS provider.

*Hyper Text Transport Protocol (http)

Responsible role indicates the role of a CSP employee who can best respond to questions about the particular control that is described.

TABLE OF CONTENTS

Access Control **25**

AC-1 Policy and Procedures (L)(M)(H)....25

AC-2 Account Management (L)(M)(H)....26

AC-2(1) Automated System Account Management (M)(H)....29

AC-2(2) Automated Temporary and Emergency Account Management (M)(H)....30

AC-2(3) Disable Accounts (M)(H)....32

AC-2(4) Automated Audit Actions (M)(H)....33

AC-2(5) Inactivity Logout (M)(H)....34

AC-2(7) Privileged User Accounts (M)(H)....35

AC-2(9) Restrictions on Use of Shared and Group Accounts (M)(H)....37

AC-2(11) Usage Conditions (H)....38

AC-2(12) Account Monitoring for Atypical Usage (M)(H)....39

AC-2(13) Disable Accounts for High-risk Individuals (M)(H)....40

AC-3 Access Enforcement (L)(M)(H)....41

AC-4 Information Flow Enforcement (M)(H)....42

AC-4(4) Flow Control of Encrypted Information (H)....43

AC-4(21) Physical or Logical Separation of Information Flows (M)(H)....45

AC-5 Separation of Duties (M)(H)....46

AC-6 Least Privilege (M)(H)....47

AC-6(1) Authorize Access to Security Functions (M)(H)....48

AC-6(2) Non-privileged Access for Nonsecurity Functions (M)(H)....49

AC-6(3) Network Access to Privileged Commands (H)....51

AC-6(5) Privileged Accounts (M)(H)..... 52
AC-6(7) Review of User Privileges (M)(H)..... 53
AC-6(8) Privilege Levels for Code Execution (H)..... 54
AC-6(9) Log Use of Privileged Functions (M)(H)..... 55
AC-6(10) Prohibit Non-privileged Users from Executing Privileged Functions (M)(H)..... 56
AC-7 Unsuccessful Logon Attempts (L)(M)(H)..... 57
AC-8 System Use Notification (L)(M)(H)..... 58
AC-10 Concurrent Session Control (H)..... 61
AC-11 Device Lock (M)(H)..... 62
AC-11(1) Pattern-hiding Displays (M)(H)..... 63
AC-12 Session Termination (M)(H)..... 64
AC-14 Permitted Actions Without Identification or Authentication (L)(M)(H)..... 65
AC-17 Remote Access (L)(M)(H)..... 66
AC-17(1) Monitoring and Control (M)(H)..... 67
AC-17(2) Protection of Confidentiality and Integrity Using Encryption (M)(H)..... 68
AC-17(3) Managed Access Control Points (M)(H)..... 69
AC-17(4) Privileged Commands and Access (M)(H)..... 70
AC-18 Wireless Access (L)(M)(H)..... 72
AC-18(1) Authentication and Encryption (M)(H)..... 73
AC-18(3) Disable Wireless Networking (M)(H)..... 74
AC-18(4) Restrict Configurations by Users (H)..... 75
AC-18(5) Antennas and Transmission Power Levels (H)..... 76
AC-19 Access Control for Mobile Devices (L)(M)(H)..... 77
AC-19(5) Full Device or Container-based Encryption (M)(H)..... 78

AC-20 Use of External Systems (L)(M)(H)..... 79
AC-20(1) Limits on Authorized Use (M)(H)..... 81
AC-20(2) Portable Storage Devices — Restricted Use (M)(H)..... 82
AC-21 Information Sharing (M)(H)..... 83
AC-22 Publicly Accessible Content (L)(M)(H)..... 84
Awareness and Training **86**
AT-1 Policy and Procedures (L)(M)(H)..... 86
AT-2 Literacy Training and Awareness (L)(M)(H)..... 88
AT-2(2) Insider Threat (L)(M)(H)..... 89
AT-2(3) Social Engineering and Mining (M)(H)..... 90
AT-3 Role-based Training (L)(M)(H)..... 91
AT-4 Training Records (L)(M)(H)..... 93
Audit and Accountability **94**
AU-1 Policy and Procedures (L)(M)(H)..... 94
AU-2 Event Logging (L)(M)(H)..... 96
AU-3 Content of Audit Records (L)(M)(H)..... 98
AU-3(1) Additional Audit Information (M)(H)..... 99
AU-4 Audit Log Storage Capacity (L)(M)(H)..... 100
AU-5 Response to Audit Logging Process Failures (L)(M)(H)..... 102
AU-5(1) Storage Capacity Warning (H)..... 103
AU-5(2) Real-time Alerts (H)..... 104
AU-6 Audit Record Review, Analysis, and Reporting (L)(M)(H)..... 105
AU-6(1) Automated Process Integration (M)(H)..... 107
AU-6(3) Correlate Audit Record Repositories (M)(H)..... 108

AU-6(4) Central Review and Analysis (H)..... 109
AU-6(5) Integrated Analysis of Audit Records (H)..... 110
AU-6(6) Correlation with Physical Monitoring (H)..... 111
AU-6(7) Permitted Actions (H)..... 112
AU-7 Audit Record Reduction and Report Generation (M)(H)..... 113
AU-7(1) Automatic Processing (M)(H)..... 114
AU-8 Time Stamps (L)(M)(H)..... 115
AU-9 Protection of Audit Information (L)(M)(H)..... 117
AU-9(2) Store on Separate Physical Systems or Components (H)..... 118
AU-9(3) Cryptographic Protection (H)..... 119
AU-9(4) Access by Subset of Privileged Users (M)(H)..... 120
AU-10 Non-repudiation (H)..... 121
AU-11 Audit Record Retention (L)(M)(H)..... 122
AU-12 Audit Record Generation (L)(M)(H)..... 123
AU-12(1) System-wide and Time-correlated Audit Trail (H)..... 125
AU-12(3) Changes by Authorized Individuals (H)..... 126
Assessment, Authorization, and Monitoring 127
CA-1 Policy and Procedures (L)(M)(H)..... 127
CA-2 Control Assessments (L)(M)(H)..... 129
CA-2(1) Independent Assessors (L)(M)(H)..... 131
CA-2(2) Specialized Assessments (H)..... 132
CA-2(3) Leveraging Results from External Organizations (M)(H)..... 133
CA-3 Information Exchange (L)(M)(H)..... 135
CA-3(6) Transfer Authorizations (H)..... 136

CA-5 Plan of Action and Milestones (L)(M)(H)..... 137
CA-6 Authorization (L)(M)(H)..... 138
CA-7 Continuous Monitoring (L)(M)(H)..... 140
CA-7(1) Independent Assessment (M)(H)..... 142
CA-7(4) Risk Monitoring (L)(M)(H)..... 143
CA-8 Penetration Testing (L)(M)(H)..... 145
CA-8(1) Independent Penetration Testing Agent or Team (M)(H)..... 146
CA-8(2) Red Team Exercises (M)(H)..... 147
CA-9 Internal System Connections (L)(M)(H)..... 148
Configuration Management **150**
CM-1 Policy and Procedures (L)(M)(H)..... 150
CM-2 Baseline Configuration (L)(M)(H)..... 152
CM-2(2) Automation Support for Accuracy and Currency (M)(H)..... 153
CM-2(3) Retention of Previous Configurations (M)(H)..... 154
CM-2(7) Configure Systems and Components for High-risk Areas (M)(H)..... 155
CM-3 Configuration Change Control (M)(H)..... 156
CM-3(1) Automated Documentation, Notification, and Prohibition of Changes (H)..... 159
CM-3(2) Testing, Validation, and Documentation of Changes (M)(H)..... 160
CM-3(4) Security and Privacy Representatives (M)(H)..... 161
CM-3(6) Cryptography Management (H)..... 162
CM-4 Impact Analyses (L)(M)(H)..... 164
CM-4(1) Separate Test Environments (H)..... 165
CM-4(2) Verification of Controls (M)(H)..... 166
CM-5 Access Restrictions for Change (L)(M)(H)..... 167

CM-5(1) Automated Access Enforcement and Audit Records (M)(H)..... 168
CM-5(5) Privilege Limitation for Production and Operation (M)(H)..... 169
CM-6 Configuration Settings (L)(M)(H)..... 170
CM-6(1) Automated Management, Application, and Verification (M)(H)..... 172
CM-6(2) Respond to Unauthorized Changes (H)..... 173
CM-7 Least Functionality (L)(M)(H)..... 174
CM-7(1) Periodic Review (M)(H)..... 176
CM-7(2) Prevent Program Execution (M)(H)..... 177
CM-7(5) Authorized Software — Allow-by-exception (M)(H)..... 178
CM-8 System Component Inventory (L)(M)(H)..... 180
CM-8(1) Updates During Installation and Removal (M)(H)..... 181
CM-8(2) Automated Maintenance (H)..... 182
CM-8(3) Automated Unauthorized Component Detection (M)(H)..... 183
CM-8(4) Accountability Information (H)..... 185
CM-9 Configuration Management Plan (M)(H)..... 186
CM-10 Software Usage Restrictions (L)(M)(H)..... 187
CM-11 User-installed Software (L)(M)(H)..... 189
CM-12 Information Location (M)(H)..... 190
CM-12(1) Automated Tools to Support Information Location (M)(H)..... 191
CM-14 Signed Components (H)..... 193
Contingency Planning **194**
CP-1 Policy and Procedures (L)(M)(H)..... 194
CP-2 Contingency Plan (L)(M)(H)..... 196
CP-2(1) Coordinate with Related Plans (M)(H)..... 198

CP-2(2) Capacity Planning (H)..... 199
CP-2(3) Resume Mission and Business Functions (M)(H)..... 200
CP-2(5) Continue Mission and Business Functions (H)..... 201
CP-2(8) Identify Critical Assets (M)(H)..... 202
CP-3 Contingency Training (L)(M)(H)..... 204
CP-3(1) Simulated Events (H)..... 205
CP-4 Contingency Plan Testing (L)(M)(H)..... 206
CP-4(1) Coordinate with Related Plans (M)(H)..... 208
CP-4(2) Alternate Processing Site (H)..... 209
CP-6 Alternate Storage Site (M)(H)..... 210
CP-6(1) Separation from Primary Site (M)(H)..... 211
CP-6(2) Recovery Time and Recovery Point Objectives (H)..... 212
CP-6(3) Accessibility (M)(H)..... 213
CP-7 Alternate Processing Site (M)(H)..... 214
CP-7(1) Separation from Primary Site (M)(H)..... 216
CP-7(2) Accessibility (M)(H)..... 217
CP-7(3) Priority of Service (M)(H)..... 218
CP-7(4) Preparation for Use (H)..... 219
CP-8 Telecommunications Services (M)(H)..... 220
CP-8(1) Priority of Service Provisions (M)(H)..... 221
CP-8(2) Single Points of Failure (M)(H)..... 222
CP-8(3) Separation of Primary and Alternate Providers (H)..... 223
CP-8(4) Provider Contingency Plan (H)..... 224
CP-9 System Backup (L)(M)(H)..... 225

CP-9(1) Testing for Reliability and Integrity (M)(H)....227
CP-9(2) Test Restoration Using Sampling (H)....228
CP-9(3) Separate Storage for Critical Information (H)....229
CP-9(5) Transfer to Alternate Storage Site (H)....231
CP-9(8) Cryptographic Protection (M)(H)....232
CP-10 System Recovery and Reconstitution (L)(M)(H)....233
CP-10(2) Transaction Recovery (M)(H)....234
CP-10(4) Restore Within Time Period (H)....235
Identification and Authentication 236
IA-1 Policy and Procedures (L)(M)(H)....236
IA-2 Identification and Authentication (Organizational Users) (L)(M)(H)....238
IA-2(1) Multi-factor Authentication to Privileged Accounts (L)(M)(H)....239
IA-2(2) Multi-factor Authentication to Non-privileged Accounts (L)(M)(H)....240
IA-2(5) Individual Authentication with Group Authentication (M)(H)....242
IA-2(6) Access to Accounts —separate Device (M)(H)....243
IA-2(8) Access to Accounts — Replay Resistant (L)(M)(H)....244
IA-2(12) Acceptance of PIV Credentials (L)(M)(H)....245
IA-3 Device Identification and Authentication (M)(H)....246
IA-4 Identifier Management (L)(M)(H)....247
IA-4(4) Identify User Status (M)(H)....249
IA-5 Authenticator Management (L)(M)(H)....250
IA-5(1) Password-based Authentication (L)(M)(H)....252
IA-5(2) Public Key-based Authentication (M)(H)....254
IA-5(6) Protection of Authenticators (M)(H)....256

IA-5(7) No Embedded Unencrypted Static Authenticators (M)(H)....257
IA-5(8) Multiple System Accounts (H)....258
IA-5(13) Expiration of Cached Authenticators (H)....259
IA-6 Authentication Feedback (L)(M)(H)....260
IA-7 Cryptographic Module Authentication (L)(M)(H)....261
IA-8 Identification and Authentication (Non-organizational Users) (L)(M)(H)....262
IA-8(1) Acceptance of PIV Credentials from Other Agencies (L)(M)(H)....263
IA-8(2) Acceptance of External Authenticators (L)(M)(H)....264
IA-8(4) Use of Defined Profiles (L)(M)(H)....265
IA-11 Re-authentication (L)(M)(H)....266
IA-12 Identity Proofing (M)(H)....268
IA-12(2) Identity Evidence (M)(H)....269
IA-12(3) Identity Evidence Validation and Verification (M)(H)....270
IA-12(4) In-person Validation and Verification (H)....271
IA-12(5) Address Confirmation (M)(H)....272
Incident Response **273**
IR-1 Policy and Procedures (L)(M)(H)....273
IR-2 Incident Response Training (L)(M)(H)....275
IR-2(1) Simulated Events (H)....276
IR-2(2) Automated Training Environments (H)....277
IR-3 Incident Response Testing (M)(H)....279
IR-3(2) Coordination with Related Plans (M)(H)....280
IR-4 Incident Handling (L)(M)(H)....281
IR-4(1) Automated Incident Handling Processes (M)(H)....283

IR-4(2) Dynamic Reconfiguration (H)..... 284
IR-4(4) Information Correlation (H)..... 285
IR-4(6) Insider Threats (H)..... 286
IR-4(11) Integrated Incident Response Team (H)..... 287
IR-5 Incident Monitoring (L)(M)(H)..... 288
IR-5(1) Automated Tracking, Data Collection, and Analysis (H)..... 289
IR-6 Incident Reporting (L)(M)(H)..... 290
IR-6(1) Automated Reporting (M)(H)..... 291
IR-6(3) Supply Chain Coordination (M)(H)..... 292
IR-7 Incident Response Assistance (L)(M)(H)..... 293
IR-7(1) Automation Support for Availability of Information and Support (M)(H)..... 294
IR-8 Incident Response Plan (L)(M)(H)..... 295
IR-9 Information Spillage Response (M)(H)..... 298
IR-9(2) Training (M)(H)..... 299
IR-9(3) Post-spill Operations (M)(H)..... 301
IR-9(4) Exposure to Unauthorized Personnel (M)(H)..... 302
Maintenance **303**
MA-1 Policy and Procedures (L)(M)(H)..... 303
MA-2 Controlled Maintenance (L)(M)(H)..... 305
MA-2(2) Automated Maintenance Activities (H)..... 306
MA-3 Maintenance Tools (M)(H)..... 308
MA-3(1) Inspect Tools (M)(H)..... 309
MA-3(2) Inspect Media (M)(H)..... 310
MA-3(3) Prevent Unauthorized Removal (M)(H)..... 311

MA-4 Nonlocal Maintenance (L)(M)(H)....312
MA-4(3) Comparable Security and Sanitization (H)....313
MA-5 Maintenance Personnel (L)(M)(H)....315
MA-5(1) Individuals Without Appropriate Access (M)(H)....316
MA-6 Timely Maintenance (M)(H)....318
Media Protection **319**
MP-1 Policy and Procedures (L)(M)(H)....319
MP-2 Media Access (L)(M)(H)....321
MP-3 Media Marking (M)(H)....322
MP-4 Media Storage (M)(H)....323
MP-5 Media Transport (M)(H)....324
MP-6 Media Sanitization (L)(M)(H)....326
MP-6(1) Review, Approve, Track, Document, and Verify (H)....327
MP-6(2) Equipment Testing (H)....328
MP-6(3) Nondestructive Techniques (H)....329
MP-7 Media Use (L)(M)(H)....331
Physical and Environmental Protection **332**
PE-1 Policy and Procedures (L)(M)(H)....332
PE-2 Physical Access Authorizations (L)(M)(H)....334
PE-3 Physical Access Control (L)(M)(H)....335
PE-3(1) System Access (H)....337
PE-4 Access Control for Transmission (M)(H)....339
PE-5 Access Control for Output Devices (M)(H)....340
PE-6 Monitoring Physical Access (L)(M)(H)....341

PE-6(1) Intrusion Alarms and Surveillance Equipment (M)(H)..... 342
PE-6(4) Monitoring Physical Access to Systems (H)..... 343
PE-8 Visitor Access Records (L)(M)(H)..... 344
PE-8(1) Automated Records Maintenance and Review (H)..... 346
PE-9 Power Equipment and Cabling (M)(H)..... 347
PE-10 Emergency Shutoff (M)(H)..... 348
PE-11 Emergency Power (M)(H)..... 349
PE-11(1) Alternate Power Supply — Minimal Operational Capability (H)..... 350
PE-12 Emergency Lighting (L)(M)(H)..... 351
PE-13 Fire Protection (L)(M)(H)..... 352
PE-13(1) Detection Systems — Automatic Activation and Notification (M)(H)..... 353
PE-13(2) Suppression Systems — Automatic Activation and Notification (M)(H)..... 354
PE-14 Environmental Controls (L)(M)(H)..... 355
PE-14(2) Monitoring with Alarms and Notifications (H)..... 357
PE-15 Water Damage Protection (L)(M)(H)..... 358
PE-15(1) Automation Support (H)..... 359
PE-16 Delivery and Removal (L)(M)(H)..... 360
PE-17 Alternate Work Site (M)(H)..... 361
PE-18 Location of System Components (H)..... 363
Planning **364**
PL-1 Policy and Procedures (L)(M)(H)..... 364
PL-2 System Security and Privacy Plans (L)(M)(H)..... 366
PL-4 Rules of Behavior (L)(M)(H)..... 368
PL-4(1) Social Media and External Site/Application Usage Restrictions (L)(M)(H)..... 369

PL-8 Security and Privacy Architectures (L)(M)(H)..... 371
PL-10 Baseline Selection (L)(M)(H)..... 372
PL-11 Baseline Tailoring (L)(M)(H)..... 373
Personnel Security **375**
PS-1 Policy and Procedures (L)(M)(H)..... 375
PS-2 Position Risk Designation (L)(M)(H)..... 376
PS-3 Personnel Screening (L)(M)(H)..... 378
PS-3(3) Information Requiring Special Protective Measures (M)(H)..... 379
PS-4 Personnel Termination (L)(M)(H)..... 380
PS-4(2) Automated Actions (H)..... 382
PS-5 Personnel Transfer (L)(M)(H)..... 383
PS-6 Access Agreements (L)(M)(H)..... 384
PS-7 External Personnel Security (L)(M)(H)..... 386
PS-8 Personnel Sanctions (L)(M)(H)..... 387
PS-9 Position Descriptions (L)(M)(H)..... 389
Risk Assessment **390**
RA-1 Policy and Procedures (L)(M)(H)..... 390
RA-2 Security Categorization (L)(M)(H)..... 392
RA-3 Risk Assessment (L)(M)(H)..... 393
RA-3(1) Supply Chain Risk Assessment (L)(M)(H)..... 395
RA-5 Vulnerability Monitoring and Scanning (L)(M)(H)..... 396
RA-5(2) Update Vulnerabilities to Be Scanned (L)(M)(H)..... 399
RA-5(3) Breadth and Depth of Coverage (M)(H)..... 400
RA-5(4) Discoverable Information (H)..... 401

RA-5(5) Privileged Access (M)(H)..... 402
RA-5(8) Review Historic Audit Logs (H)..... 403
RA-5(11) Public Disclosure Program (L)(M)(H)..... 405
RA-7 Risk Response (L)(M)(H)..... 406
RA-9 Criticality Analysis (M)(H)..... 407
System and Services Acquisition **408**
SA-1 Policy and Procedures (L)(M)(H)..... 408
SA-2 Allocation of Resources (L)(M)(H)..... 410
SA-3 System Development Life Cycle (L)(M)(H)..... 411
SA-4 Acquisition Process (L)(M)(H)..... 412
SA-4(1) Functional Properties of Controls (M)(H)..... 414
SA-4(2) Design and Implementation Information for Controls (M)(H)..... 415
SA-4(5) System, Component, and Service Configurations (H)..... 417
SA-4(9) Functions, Ports, Protocols, and Services in Use (M)(H)..... 418
SA-4(10) Use of Approved PIV Products (L)(M)(H)..... 419
SA-5 System Documentation (L)(M)(H)..... 420
SA-8 Security and Privacy Engineering Principles (L)(M)(H)..... 422
SA-9 External System Services (L)(M)(H)..... 423
SA-9(1) Risk Assessments and Organizational Approvals (M)(H)..... 424
SA-9(2) Identification of Functions, Ports, Protocols, and Services (M)(H)..... 425
SA-9(5) Processing, Storage, and Service Location (M)(H)..... 426
SA-10 Developer Configuration Management (M)(H)..... 428
SA-11 Developer Testing and Evaluation (M)(H)..... 429
SA-11(1) Static Code Analysis (M)(H)..... 431

SA-11(2) Threat Modeling and Vulnerability Analyses (M)(H)....432
SA-15 Development Process, Standards, and Tools (M)(H)....434
SA-15(3) Criticality Analysis (M)(H)....435
SA-16 Developer-provided Training (H)....437
SA-17 Developer Security and Privacy Architecture and Design (H)....438
SA-21 Developer Screening (H)....439
SA-22 Unsupported System Components (L)(M)(H)....440
System and Communications Protection 442
SC-1 Policy and Procedures (L)(M)(H)....442
SC-2 Separation of System and User Functionality (M)(H)....443
SC-3 Security Function Isolation (H)....444
SC-4 Information in Shared System Resources (M)(H)....445
SC-5 Denial-of-service Protection (L)(M)(H)....446
SC-7 Boundary Protection (L)(M)(H)....448
SC-7(3) Access Points (M)(H)....449
SC-7(4) External Telecommunications Services (M)(H)....450
SC-7(5) Deny by Default — Allow by Exception (M)(H)....452
SC-7(7) Split Tunneling for Remote Devices (M)(H)....453
SC-7(8) Route Traffic to Authenticated Proxy Servers (M)(H)....454
SC-7(10) Prevent Exfiltration (H)....456
SC-7(12) Host-based Protection (M)(H)....457
SC-7(18) Fail Secure (M)(H)....458
SC-7(20) Dynamic Isolation and Segregation (H)....459
SC-7(21) Isolation of System Components (H)....460

SC-8 Transmission Confidentiality and Integrity (L)(M)(H)....461
SC-8(1) Cryptographic Protection (L)(M)(H)....463
SC-10 Network Disconnect (M)(H)....465
SC-12 Cryptographic Key Establishment and Management (L)(M)(H)....466
SC-12(1) Availability (H)....467
SC-13 Cryptographic Protection (L)(M)(H)....468
SC-15 Collaborative Computing Devices and Applications (L)(M)(H)....471
SC-17 Public Key Infrastructure Certificates (M)(H)....472
SC-18 Mobile Code (M)(H)....473
SC-20 Secure Name/Address Resolution Service (Authoritative Source) (L)(M)(H)....474
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (L)(M)(H). 476
SC-22 Architecture and Provisioning for Name/Address Resolution Service (L)(M)(H)....477
SC-23 Session Authenticity (M)(H)....478
SC-24 Fail in Known State (H)....479
SC-28 Protection of Information at Rest (L)(M)(H)....481
SC-28(1) Cryptographic Protection (L)(M)(H)....482
SC-39 Process Isolation (L)(M)(H)....484
SC-45 System Time Synchronization (M)(H)....485
SC-45(1) Synchronization with Authoritative Time Source (M)(H)....486
System and Information Integrity 487
SI-1 Policy and Procedures (L)(M)(H)....487
SI-2 Flaw Remediation (L)(M)(H)....489
SI-2(2) Automated Flaw Remediation Status (M)(H)....490

SI-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions (M)(H)..... 492
SI-3 Malicious Code Protection (L)(M)(H)..... 493
SI-4 System Monitoring (L)(M)(H)..... 495
SI-4(1) System-wide Intrusion Detection System (M)(H)..... 497
SI-4(2) Automated Tools and Mechanisms for Real-time Analysis (M)(H)..... 498
SI-4(4) Inbound and Outbound Communications Traffic (M)(H)..... 499
SI-4(5) System-generated Alerts (M)(H)..... 500
SI-4(10) Visibility of Encrypted Communications (H)..... 501
SI-4(11) Analyze Communications Traffic Anomalies (H)..... 502
SI-4(12) Automated Organization-generated Alerts (H)..... 503
SI-4(14) Wireless Intrusion Detection (H)..... 505
SI-4(16) Correlate Monitoring Information (M)(H)..... 506
SI-4(18) Analyze Traffic and Covert Exfiltration (M)(H)..... 507
SI-4(19) Risk for Individuals (H)..... 508
SI-4(20) Privileged Users (H)..... 509
SI-4(22) Unauthorized Network Services (H)..... 510
SI-4(23) Host-based Devices (M)(H)..... 511
SI-5 Security Alerts, Advisories, and Directives (L)(M)(H)..... 512
SI-5(1) Automated Alerts and Advisories (H)..... 514
SI-6 Security and Privacy Function Verification (M)(H)..... 515
SI-7 Software, Firmware, and Information Integrity (M)(H)..... 517
SI-7(1) Integrity Checks (M)(H)..... 518
SI-7(2) Automated Notifications of Integrity Violations (H)..... 519
SI-7(5) Automated Response to Integrity Violations (H)..... 520

SI-7(7) Integration of Detection and Response (M)(H)....521
SI-7(15) Code Authentication (H)....522
SI-8 Spam Protection (M)(H)....523
SI-8(2) Automatic Updates (M)(H)....525
SI-10 Information Input Validation (M)(H)....526
SI-11 Error Handling (M)(H)....527
SI-12 Information Management and Retention (L)(M)(H)....528
SI-16 Memory Protection (M)(H)....529
Supply Chain Risk Management 530
SR-1 Policy and Procedures (L)(M)(H)....530
SR-2 Supply Chain Risk Management Plan (L)(M)(H)....532
SR-2(1) Establish SCRM Team (L)(M)(H)....533
SR-3 Supply Chain Controls and Processes (L)(M)(H)....535
SR-5 Acquisition Strategies, Tools, and Methods (L)(M)(H)....536
SR-6 Supplier Assessments and Reviews (M)(H)....537
SR-8 Notification Agreements (L)(M)(H)....539
SR-9 Tamper Resistance and Detection (H)....540
SR-9(1) Multiple Stages of System Development Life Cycle (H)....541
SR-10 Inspection of Systems or Components (L)(M)(H)....542
SR-11 Component Authenticity (L)(M)(H)....543
SR-11(1) Anti-counterfeit Training (L)(M)(H)....544
SR-11(2) Configuration Control for Component Service and Repair (L)(M)(H)....545
SR-12 Component Disposal (L)(M)(H)....547

Access Control

AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] access control policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

   1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AC-1 Control Summary Information
Responsible Role:
Parameter AC-1(a):
Parameter AC-1(a)(1):

Parameter AC-1(b):
Parameter AC-1(c)(1)-1:
Parameter AC-1(c)(1)-2:
Parameter AC-1(c)(2)-1:
Parameter AC-1(c)(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)

AC-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;

d. Specify:

   1. Authorized users of the system;

   2. Group and role membership; and

   3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;

e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];

g. Monitor the use of accounts;

h. Notify account managers and [Assignment: organization-defined personnel or roles] within:

   1. [FedRAMP Assignment: twenty-four (24) hours] when accounts are no longer required;

   2. [FedRAMP Assignment: eight (8) hours] when users are terminated or transferred; and

   3. [FedRAMP Assignment: eight (8) hours] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

   1. A valid access authorization;

2. Intended system usage; and

3. [Assignment: organization-defined attributes (as required)];

j. Review accounts for compliance with account management requirements [FedRAMP Assignment: monthly for privileged accessed, every six (6) months for non-privileged access];

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

AC-2 Control Summary Information
Responsible Role:
Parameter AC-2(c):
Parameter AC-2(d)(3):
Parameter AC-2(e):
Parameter AC-2(f):
Parameter AC-2(h):
Parameter AC-2(h)(1):
Parameter AC-2(h)(2):
Parameter AC-2(h)(3):
Parameter AC-2(i)(3):
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 FedRAMP 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:
Part l:

AC-2(1) Automated System Account Management (M)(H)

Support the management of system accounts using [Assignment: organization-defined automated mechanisms].

AC-2(1) Control Summary Information
Responsible Role:
Parameter AC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

AC-2(2) Automated Temporary and Emergency Account Management (M)(H)

Automatically [FedRAMP Assignment: disables] temporary and emergency accounts after [FedRAMP Assignment: no more than twenty-four (24) hours from last use].

AC-2(2) Control Summary Information
Responsible Role:
Parameter AC-2(2)-1:
Parameter AC-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(2) What is the solution and how is it implemented?

AC-2(3) Disable Accounts (M)(H)

Disable accounts within [FedRAMP Assignment: twenty-four (24) hours for user accounts] when the accounts:

a. Have expired;

b. Are no longer associated with a user or individual;

c. Are in violation of organizational policy; or

d. Have been inactive for [FedRAMP Assignment: thirty-five (35) days (See additional requirements and guidance.)].

AC-2 (3) Additional FedRAMP Requirements and Guidance:

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP https://public.cyber.mil/dccs/.

Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

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

AC-2(3) Control Summary Information
Responsible Role:
Parameter AC-2(3):
Parameter AC-2(3)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(3) What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

AC-2(4) Automated Audit Actions (M)(H)

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AC-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(4) What is the solution and how is it implemented?

AC-2(5) Inactivity Logout (M)(H)

Require that users log out when [FedRAMP Assignment: inactivity is anticipated to exceed fifteen (15) minutes].

AC-2 (5) Additional FedRAMP Requirements and Guidance:

Guidance: Should use a shorter timeframe than AC-12.

AC-2(5) Control Summary Information
Responsible Role:
Parameter AC-2(5):

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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(5) What is the solution and how is it implemented?

AC-2(7) Privileged User Accounts (M)(H)

(a) Establish and administer privileged user accounts in accordance with [Selection: Assignment: a role-based access scheme; an attribute-based access scheme];

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

AC-2(7) Control Summary Information
Responsible Role:
Parameter AC-2(7)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(7) What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

AC-2(9) Restrictions on Use of Shared and Group Accounts (M)(H)

Only permit the use of shared and group accounts that meet [FedRAMP Assignment: organization-defined need with justification statement that explains why such accounts are necessary].

AC-2 (9) Additional FedRAMP Requirements and Guidance:

Requirement: Required if shared/group accounts are deployed.

AC-2(9) Control Summary Information
Responsible Role:
Parameter AC-2(9):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(9) What is the solution and how is it implemented?

AC-2(11) Usage Conditions (H)

Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].

AC-2(11) Control Summary Information
Responsible Role:
Parameter AC-2(11)-1:
Parameter AC-2(11)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(11) What is the solution and how is it implemented?

AC-2(12) Account Monitoring for Atypical Usage (M)(H)

(a) Monitor system accounts for [Assignment: organization-defined atypical usage]; and

(b) Report atypical usage of system accounts to [FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization].

AC-2 (12) Additional FedRAMP Requirements and Guidance:

(a) Requirement: Required for privileged accounts.

(b) Requirement: Required for privileged accounts.

AC-2(12) Control Summary Information
Responsible Role:
Parameter AC-2(12)(a):
Parameter AC-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(12) What is the solution and how is it implemented?
Part a:
Part b:

AC-2(13) Disable Accounts for High-risk Individuals (M)(H)

Disable accounts of individuals within [FedRAMP Assignment: one (1) hour] of discovery of [Assignment: organization-defined significant risks].

AC-2(13) Control Summary Information
Responsible Role:
Parameter AC-2(13)-1:
Parameter AC-2(13)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-2(13) What is the solution and how is it implemented?

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

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-3 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

AC-4 Information Flow Enforcement (M)(H)

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

AC-4 Control Summary Information
Responsible Role:
Parameter AC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-4 What is the solution and how is it implemented?

AC-4(4) Flow Control of Encrypted Information (H)

Prevent encrypted information from bypassing [FedRAMP Assignment: intrusion detection mechanisms] by [Selection (one-or-more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information].

AC-4 (4) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Feder

al-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).

AC-4(4) Control Summary Information
Responsible Role:
Parameter AC-4(4)-1:
Parameter AC-4(4)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-4(4) What is the solution and how is it implemented?

AC-4(21) Physical or Logical Separation of Information Flows (M)(H)

Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

AC-4(21) Control Summary Information
Responsible Role:
Parameter AC-4(21)-1:
Parameter AC-4(21)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-4(21) What is the solution and how is it implemented?

AC-5 Separation of Duties (M)(H)

a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and

b. Define system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP.

AC-5 Control Summary Information
Responsible Role:
Parameter AC-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-5 What is the solution and how is it implemented?
Part a:
Part b:

AC-6 Least Privilege (M)(H)

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6 What is the solution and how is it implemented?

AC-6(1) Authorize Access to Security Functions (M)(H)

Authorize access for [Assignment: organization-defined individuals or roles] to:

(a) [FedRAMP Assignment: all functions not publicly accessible]; and

(b) [FedRAMP Assignment: all security-relevant information not publicly available].

AC-6(1) Control Summary Information
Responsible Role:
Parameter AC-6(1):
Parameter AC-6(1)(a):
Parameter AC-6(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(1) What is the solution and how is it implemented?
Part a:
Part b:

AC-6(2) Non-privileged Access for Nonsecurity Functions (M)(H)

Require that users of system accounts (or roles) with access to [FedRAMP Assignment: all security functions] use non-privileged accounts or roles, when accessing nonsecurity functions.

AC-6 (2) Additional FedRAMP Requirements and Guidance:

Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

AC-6(2) Control Summary Information
Responsible Role:
Parameter AC-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(2) What is the solution and how is it implemented?

AC-6(3) Network Access to Privileged Commands (H)

Authorize network access to [FedRAMP Assignment: all privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.

AC-6(3) Control Summary Information
Responsible Role:
Parameter AC-6(3)-1:
Parameter AC-6(3)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(3) What is the solution and how is it implemented?

AC-6(5) Privileged Accounts (M)(H)

Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

AC-6(5) Control Summary Information

Responsible Role:
Parameter AC-6(5):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(5) What is the solution and how is it implemented?

AC-6(7) Review of User Privileges (M)(H)

(a) Review [FedRAMP Assignment: at a minimum, annually] the privileges assigned to [FedRAMP Assignment: all users with privileges] to validate the need for such privileges; and

(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-6(7) Control Summary Information
Responsible Role:
Parameter AC-6(7)(a)-1:
Parameter AC-6(7)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(7) What is the solution and how is it implemented?
Part a:
Part b:

AC-6(8) Privilege Levels for Code Execution (H)

Prevent the following software from executing at higher privilege levels than users executing the software: [FedRAMP Assignment: any software except software explicitly documented].

AC-6(8) Control Summary Information
Responsible Role:
Parameter AC-6(8):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(8) What is the solution and how is it implemented?

AC-6(9) Log Use of Privileged Functions (M)(H)

Log the execution of privileged functions.

AC-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(9) What is the solution and how is it implemented?

AC-6(10) Prohibit Non-privileged Users from Executing Privileged Functions (M)(H)

Prevent non-privileged users from executing privileged functions.

AC-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-6(10) What is the solution and how is it implemented?

AC-7 Unsuccessful Logon Attempts (L)(M)(H)

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection (one-or-more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

AC-7 Additional FedRAMP Requirements and Guidance:

Requirement: In alignment with NIST SP 800-63B.

AC-7 Control Summary Information
Responsible Role:
Parameter AC-7(a)-1:
Parameter AC-7(a)-2:
Parameter AC-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 FedRAMP 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)

a. Display [FedRAMP Assignment: see additional Requirements and Guidance] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

   1. Users are accessing a U.S. Government system;
   2. System usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
   4. Use of the system indicates consent to monitoring and recording;

b. Retain 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 system; and

c. For publicly accessible systems:

   1. Display system use information [FedRAMP Assignment: see additional Requirements and Guidance], before granting further access to the publicly accessible system.
   2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Include a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

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

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 is 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 FedRAMP 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:

AC-10 Concurrent Session Control (H)

Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access].

AC-10 Control Summary Information
Responsible Role:

Parameter AC-10-1:
Parameter AC-10-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-10 What is the solution and how is it implemented?

AC-11 Device Lock (M)(H)

a. Prevent further access to the system by [Selection (one-or-more): initiating a device lock after [FedRAMP Assignment: fifteen (15) minutes of inactivity]; requiring the user to initiate a device lock before leaving the system unattended]; and

b. Retain the device lock until the user re-establishes access using established identification and authentication procedures.

AC-11 Control Summary Information
Responsible Role:
Parameter AC-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-11 What is the solution and how is it implemented?
Part a:
Part b:

AC-11(1) Pattern-hiding Displays (M)(H)

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

AC-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-11(1) What is the solution and how is it implemented?

AC-12 Session Termination (M)(H)

Automatically terminate a user session after [Assignment: organization-defined conditions, or trigger events requiring session disconnect].

AC-12 Control Summary Information
Responsible Role:
Parameter AC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-12 What is the solution and how is it implemented?

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

a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the 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 FedRAMP 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)

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

AC-17 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

AC-17(1) Monitoring and Control (M)(H)

Employ automated mechanisms to monitor and control remote access methods.

AC-17(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-17(1) What is the solution and how is it implemented?

AC-17(2) Protection of Confidentiality and Integrity Using Encryption (M)(H)

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-17(2) What is the solution and how is it implemented?

AC-17(3) Managed Access Control Points (M)(H)

Route remote accesses through authorized and managed network access control points.

AC-17(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-17(3) What is the solution and how is it implemented?

AC-17(4) Privileged Commands and Access (M)(H)

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; and

(b) Document the rationale for remote access in the security plan for the system.

AC-17(4) Control Summary Information
Responsible Role:
Parameter AC-17(4)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-17(4) What is the solution and how is it implemented?
Part a:
Part b:

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

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the 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 FedRAMP 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-18(1) Authentication and Encryption (M)(H)

Protect wireless access to the system using authentication of [Selection (one-or-more): users; devices] and encryption.

AC-18(1) Control Summary Information
Responsible Role:
Parameter AC-18(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-18(1) What is the solution and how is it implemented?

AC-18(3) Disable Wireless Networking (M)(H)

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

AC-18(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-18(3) What is the solution and how is it implemented?

AC-18(4) Restrict Configurations by Users (H)

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

AC-18(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-18(4) What is the solution and how is it implemented?

AC-18(5) Antennas and Transmission Power Levels (H)

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

AC-18(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-18(5) What is the solution and how is it implemented?

AC-19 Access Control for Mobile Devices (L)(M)(H)

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational 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 FedRAMP 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-19(5) Full Device or Container-based Encryption (M)(H)

Employ [Selection: Assignment: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

AC-19(5) Control Summary Information
Responsible Role:

Parameter AC-19(5)-1:
Parameter AC-19(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-19(5) What is the solution and how is it implemented?

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

a. [Selection (one-or-more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

   1. Access the system from external systems; and

   2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of [Assignment: organizationally-defined types of external systems].

AC-20 Additional FedRAMP Requirements and Guidance:

Guidance: The interrelated controls of AC-20, CA-3, and SA-9 should be differentiated as follows:

AC-20 describes system access to and from external systems.

CA-3 describes documentation of an agreement between the respective system owners when data is exchanged between the CSO and an external system.

SA-9 describes the responsibilities of external system owners. These responsibilities would typically be captured in the agreement required by CA-3.

AC-20 Control Summary Information
Responsible Role:
Parameter AC-20(a):
Parameter AC-20(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 FedRAMP 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-20(1) Limits on Authorized Use (M)(H)

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AC-20(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-20(1) What is the solution and how is it implemented?
Part a:

Part b:

AC-20(2) Portable Storage Devices — Restricted Use (M)(H)

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].

AC-20(2) Control Summary Information
Responsible Role:
Parameter AC-20(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-20(2) What is the solution and how is it implemented?

AC-21 Information Sharing (M)(H)

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and

b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.

AC-21 Control Summary Information
Responsible Role:
Parameter AC-21(a):
Parameter AC-21(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AC-21 What is the solution and how is it implemented?
Part a:
Part b:

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

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [FedRAMP Assignment: at least quarterly] and remove such information, if discovered.

AC-22 Control Summary Information
Responsible Role:
Parameter AC-22(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 FedRAMP 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-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] awareness and training policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

   1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AT-1 Control Summary Information
Responsible Role:
Parameter AT-1(a):
Parameter AT-1(a)(1):
Parameter AT-1(b):
Parameter AT-1(c)(1)-1:
Parameter AT-1(c)(1)-2:
Parameter AT-1(c)(2)-1:
Parameter AT-1(c)(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)

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

AT-2 Literacy Training and Awareness (L)(M)(H)

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

   1. As part of initial training for new users and [FedRAMP Assignment: at least annually] thereafter; and

   2. When required by system changes or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];

c. Update literacy training and awareness content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

AT-2 Control Summary Information
Responsible Role:
Parameter AT-2(a)(1):
Parameter AT-2(a)(2):
Parameter AT-2(b):

Parameter AT-2(c)-1:
Parameter AT-2(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 FedRAMP 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:
Part d:

AT-2(2) Insider Threat (L)(M)(H)

Provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-2(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 FedRAMP Authorization for [Click here to enter text] Date of Authorization

AT-2(2) What is the solution and how is it implemented?

AT-2(3) Social Engineering and Mining (M)(H)

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

AT-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AT-2(3) What is the solution and how is it implemented?

AT-3 Role-based Training (L)(M)(H)

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:

   1. Before authorizing access to the system, information, or performing assigned duties, and [FedRAMP Assignment: at least annually] thereafter; and

   2. When required by system changes;

b. Update role-based training content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.

AT-3 Control Summary Information
Responsible Role:
Parameter AT-3(a):
Parameter AT-3(a)(1):
Parameter AT-3(b)-1:
Parameter AT-3(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 FedRAMP 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 Training Records (L)(M)(H)

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [FedRAMP Assignment: five (5) years or 5 years after completion of a specific training program].

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 FedRAMP 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-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] audit and accountability policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and
2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AU-1 Control Summary Information
Responsible Role:
Parameter AU-1(a):
Parameter AU-1(a)(1):
Parameter AU-1(b):
Parameter AU-1(c)(1)-1:
Parameter AU-1(c)(1)-2:
Parameter AU-1(c)(2)-1:
Parameter AU-1(c)(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)

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

AU-2 Event Logging (L)(M)(H)

a. Identify the types of events that the system is capable of logging in support of the audit function: [FedRAMP 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];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2a to be audited continually for each identified event.];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [FedRAMP Assignment: annually and whenever there is a change in the threat environment].

AU-2 Additional FedRAMP Requirements and Guidance:

(e) Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

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(c):
Parameter AU-2(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 FedRAMP 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:
Part e:

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

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3 Control Summary Information
Responsible Role:
Implementation Status (check all that apply):

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

Part f:

AU-3(1) Additional Audit Information (M)(H)

Generate audit records containing the following additional information: [FedRAMP Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands].

AU-3 (1) Additional FedRAMP Requirements and Guidance:

Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

AU-3(1) Control Summary Information
Responsible Role:
Parameter AU-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-3(1) What is the solution and how is it implemented?

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

Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention 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 FedRAMP 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 Logging Process Failures (L)(M)(H)

a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and

b. Take the following additional actions: [FedRAMP Assignment: overwrite oldest record].

AU-5 Control Summary Information
Responsible Role:
Parameter AU-5(a)-1:

Parameter AU-5(a)-2:
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 FedRAMP 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-5(1) Storage Capacity Warning (H)

Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [FedRAMP Assignment: 75%, or one month before expected negative impact] of repository maximum audit log storage capacity.

AU-5(1) Control Summary Information
Responsible Role:
Parameter AU-5(1)-1:
Parameter AU-5(1)-2:
Parameter AU-5(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-5(1) What is the solution and how is it implemented?

AU-5(2) Real-time Alerts (H)

Provide an alert within [FedRAMP Assignment: real-time] to [FedRAMP Assignment: service provider personnel with authority to address failed audit events] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].

AU-5(2) Control Summary Information
Responsible Role:
Parameter AU-5(2)-1:
Parameter AU-5(2)-2:
Parameter AU-5(2)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-5(2) What is the solution and how is it implemented?

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

a. Review and analyze system audit records [FedRAMP Assignment: at least weekly] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;

b. Report findings to [Assignment: organization-defined personnel or roles]; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6 Additional FedRAMP Requirements and Guidance:

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

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 FedRAMP 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:
Part c:

AU-6(1) Automated Process Integration (M)(H)

Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].

AU-6(1) Control Summary Information
Responsible Role:
Parameter AU-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-6(1) What is the solution and how is it implemented?

AU-6(3) Correlate Audit Record Repositories (M)(H)

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-6(3) What is the solution and how is it implemented?

AU-6(4) Central Review and Analysis (H)

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

AU-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-6(4) What is the solution and how is it implemented?

AU-6(5) Integrated Analysis of Audit Records (H)

Integrate analysis of audit records with analysis of [FedRAMP Assignment: Selection (one-or-more): vulnerability scanning information; performance data; information system monitoring information; penetration test data; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

AU-6(5) Control Summary Information

Responsible Role:
Parameter AU-6(5):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-6(5) What is the solution and how is it implemented?

AU-6(6) Correlation with Physical Monitoring (H)

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

AU-6 (6) Additional FedRAMP Requirements and Guidance:

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

AU-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-6(6) What is the solution and how is it implemented?

AU-6(7) Permitted Actions (H)

Specify the permitted actions for each [FedRAMP Assignment: information system process; role; user] associated with the review, analysis, and reporting of audit record information.

AU-6(7) Control Summary Information
Responsible Role:
Parameter AU-6(7):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-6(7) What is the solution and how is it implemented?

AU-7 Audit Record Reduction and Report Generation (M)(H)

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

AU-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-7 What is the solution and how is it implemented?
Part a:
Part b:

AU-7(1) Automatic Processing (M)(H)

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].

AU-7(1) Control Summary Information
Responsible Role:
Parameter AU-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-7(1) What is the solution and how is it implemented?

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

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet [FedRAMP Assignment: one second granularity of time measurement] and that use Coordinated Universal Time, have a fixed

local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

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 FedRAMP 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)

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.

AU-9 Control Summary Information
Responsible Role:
Parameter AU-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-9 What is the solution and how is it implemented?
Part a:
Part b:

AU-9(2) Store on Separate Physical Systems or Components (H)

Store audit records [FedRAMP Assignment: at least weekly] in a repository that is part of a physically different system or system component than the system or component being audited.

AU-9(2) Control Summary Information
Responsible Role:
Parameter AU-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-9(2) What is the solution and how is it implemented?

AU-9(3) Cryptographic Protection (H)

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

AU-9 (3) Additional FedRAMP Requirements and Guidance:

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

AU-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-9(3) What is the solution and how is it implemented?

AU-9(4) Access by Subset of Privileged Users (M)(H)

Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].

AU-9(4) Control Summary Information

Responsible Role:
Parameter AU-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-9(4) What is the solution and how is it implemented?

AU-10 Non-repudiation (H)

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [FedRAMP Assignment: minimum actions including the addition, modification, deletion, approval, sending, or receiving of data].

AU-10 Control Summary Information
Responsible Role:
Parameter AU-10:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-10 What is the solution and how is it implemented?

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

Retain audit records for [FedRAMP Assignment: a time period in compliance with M-21-31] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

Guidance: The service provider is encouraged to align with M-21-31 where possible.

Requirement: The service provider retains audit records online for at least ninety (90) days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf)

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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

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

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [FedRAMP Assignment: all information system and network components where audit capability is deployed/available];

b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record 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 FedRAMP 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:

AU-12(1) System-wide and Time-correlated Audit Trail (H)

Compile audit records from [FedRAMP Assignment: all network, data storage, and computing devices] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

AU-12(1) Control Summary Information
Responsible Role:
Parameter AU-12(1)-1:
Parameter AU-12(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-12(1) What is the solution and how is it implemented?

AU-12(3) Changes by Authorized Individuals (H)

Provide and implement the capability for [FedRAMP Assignment: service provider-defined individuals or roles with audit configuration responsibilities] to change the logging to be performed on [FedRAMP Assignment: all network, data storage, and computing devices] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].

AU-12(3) Control Summary Information
Responsible Role:
Parameter AU-12(3)-1:
Parameter AU-12(3)-2:
Parameter AU-12(3)-3:
Parameter AU-12(3)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

AU-12(3) What is the solution and how is it implemented?

Assessment, Authorization, and Monitoring

CA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

   1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

CA-1 Control Summary Information
Responsible Role:

Parameter CA-1(a):
Parameter CA-1(a)(1):
Parameter CA-1(b):
Parameter CA-1(c)(1)-1:
Parameter CA-1(c)(1)-2:
Parameter CA-1(c)(2)-1:
Parameter CA-1(c)(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)

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

Part b:
Part c:

CA-2 Control Assessments (L)(M)(H)

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

   1. Controls and control enhancements under assessment;

   2. Assessment procedures to be used to determine control effectiveness; and

   3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation [FedRAMP 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 and privacy

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to [FedRAMP Assignment: individuals or roles to include FedRAMP PMO].

CA-2 Additional FedRAMP Requirements and Guidance:

Guidance: Reference FedRAMP Annual Assessment Guidance.

CA-2 Control Summary Information

Responsible Role:
Parameter CA-2(d):
Parameter CA-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 FedRAMP 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:
Part e:
Part f:

CA-2(1) Independent Assessors (L)(M)(H)

Employ independent assessors or assessment teams to conduct control assessments.

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

Requirement: For JAB Authorization, must use an accredited 3PAO.

CA-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CA-2(2) Specialized Assessments (H)

Include as part of control assessments [FedRAMP Assignment: at least annually], [Selection: [announced; unannounced], [Selection (one-or-more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].

CA-2 (2) Additional FedRAMP Requirements and Guidance:

Requirement: To include 'announced', 'vulnerability scanning'.

CA-2(2) Control Summary Information
Responsible Role:
Parameter CA-2(2)-1:
Parameter CA-2(2)-2:
Parameter CA-2(2)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CA-2(3) Leveraging Results from External Organizations (M)(H)

Leverage the results of control assessments performed by [FedRAMP Assignment: any FedRAMP Accredited 3PAO] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].

CA-2(3) Control Summary Information
Responsible Role:
Parameter CA-2(3)-1:
Parameter CA-2(3)-2:
Parameter CA-2(3)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CA-2(3) What is the solution and how is it implemented?

CA-3 Information Exchange (L)(M)(H)

a. Approve and manage the exchange of information between the system and other systems using [Selection (one-or-more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements, [Assignment: organization-defined type of agreement]];

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements [FedRAMP Assignment: at least annually and on input from JAB/AO].

CA-3 Control Summary Information
Responsible Role:
Parameter CA-3(a):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CA-3 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

CA-3(6) Transfer Authorizations (H)

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

CA-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CA-3(6) What is the solution and how is it implemented?

CA-5 Plan of Action and Milestones (L)(M)(H)

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted

during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [FedRAMP Assignment: at least monthly] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Guidance: Reference FedRAMP-POAM-Template

Requirement: POA&Ms must be provided at least monthly.

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 FedRAMP 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 Authorization (L)(M)(H)

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

   1. Accepts the use of common controls inherited by the system; and

   2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; and

e. Update the authorizations [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs].

CA-6 Additional FedRAMP Requirements and Guidance:

(e) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F and according to FedRAMP Significant Change Policies and Procedures. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

CA-6 Control Summary Information
Responsible Role:
Parameter CA-6(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 FedRAMP 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:
Part d:
Part e:

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

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];

b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to [FedRAMP Assignment: to include JAB/AO].[Assignment: organization-defined frequency]

CA-7 Additional FedRAMP Requirements and Guidance:

Guidance: FedRAMP does not provide a template for the Continuous Monitoring Plan. CSPs should reference the FedRAMP Continuous Monitoring Strategy Guide when developing the Continuous Monitoring Plan.

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

Requirement: CSOs with more than one agency ATO must implement a collaborative Continuous Monitoring (ConMon) approach described in the FedRAMP Guide for Multi-Agency Continuous Monitoring. This requirement applies to CSOs authorized via the Agency path as each agency customer is responsible for performing ConMon oversight. It does not apply to CSOs authorized via the JAB path because the JAB performs ConMon oversight.

CA-7 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 FedRAMP 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(1) Independent Assessment (M)(H)

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

CA-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CA-7(1) What is the solution and how is it implemented?

CA-7(4) Risk Monitoring (L)(M)(H)

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

CA-7(4) Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CA-7(4) What is the solution and how is it implemented?
Part a:
Part b:
Part c:

CA-8 Penetration Testing (L)(M)(H)

Conduct penetration testing [FedRAMP Assignment: at least annually] on [Assignment: organization-defined systems or system components].

CA-8 Additional FedRAMP Requirements and Guidance:

Guidance: Reference the FedRAMP Penetration Test Guidance.

CA-8 Control Summary Information
Responsible Role:
Parameter CA-8-1:
Parameter CA-8-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CA-8 What is the solution and how is it implemented?

CA-8(1) Independent Penetration Testing Agent or Team (M)(H)

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

CA-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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CA-8(2) Red Team Exercises (M)(H)

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].

CA-8(2) Additional FedRAMP Requirements and Guidance:

Guidance: See the FedRAMP Documents page > Penetration Test Guidance https://www.FedRAMP.gov/documents/

CA-8(2) Control Summary Information
Responsible Role:
Parameter CA-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

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

a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after [Assignment: organization-defined conditions]; and

d. Review [FedRAMP Assignment: at least annually] the continued need for each internal connection.

CA-9 Control Summary Information
Responsible Role:
Parameter CA-9(a):
Parameter CA-9(c):
Parameter CA-9(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 FedRAMP 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:
Part c:
Part d:

Configuration Management

CM-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] configuration management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

CM-1 Control Summary Information
Responsible Role:
Parameter CM-1(a):
Parameter CM-1(a)(1):
Parameter CM-1(b):
Parameter CM-1(c)(1)-1:
Parameter CM-1(c)(1)-2:
Parameter CM-1(c)(2)-1:
Parameter CM-1(c)(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)

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

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

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [FedRAMP Assignment: at least annually and when a significant change occurs];

2. When required due to [FedRAMP Assignment: to include when directed by the JAB]; and

3. When system components are installed or upgraded.

CM-2 Additional FedRAMP Requirements and Guidance:

(b)(1) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

CM-2 Control Summary Information
Responsible Role:
Parameter CM-2(b)(1):
Parameter CM-2(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 FedRAMP Authorization for [Click here to enter text] Date of Authorization

CM-2 What is the solution and how is it implemented?
Part a:
Part b:

CM-2(2) Automation Support for Accuracy and Currency (M)(H)

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].

CM-2(2) Control Summary Information
Responsible Role:
Parameter CM-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CM-2(3) Retention of Previous Configurations (M)(H)

Retain [FedRAMP Assignment: organization-defined number of previous versions of baseline configurations of the previously approved baseline configuration of IS components] of previous versions of baseline configurations of the system to support rollback.

CM-2(3) Control Summary Information
Responsible Role:
Parameter CM-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-2(3) What is the solution and how is it implemented?

CM-2(7) Configure Systems and Components for High-risk Areas (M)(H)

(a) Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].

CM-2(7) Control Summary Information

Responsible Role:
Parameter CM-2(7)(a)-1:
Parameter CM-2(7)(a)-2:
Parameter CM-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-2(7) What is the solution and how is it implemented?

Part a:
Part b:

CM-3 Configuration Change Control (M)(H)

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one-or-more): organization-defined frequency; when [Assignment: organization-defined configuration change conditions]].

CM-3 Additional FedRAMP Requirements and Guidance:

(e) Guidance: In accordance with record retention policies and procedures.

Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO.

CM-3 Control Summary Information
Responsible Role:
Parameter CM-3(e):
Parameter CM-3(g)-1:
Parameter CM-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CM-3(1) Automated Documentation, Notification, and Prohibition of Changes (H)

Use [Assignment: organization-defined automated mechanisms] to:

(a) Document proposed changes to the system;

(b) Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval;

(c) Highlight proposed changes to the system that have not been approved or disapproved within [FedRAMP Assignment: organization agreed upon time period];

(d) Prohibit changes to the system until designated approvals are received;

(e) Document all changes to the system; and

(f) Notify [FedRAMP Assignment: organization defined configuration management approval authorities] when approved changes to the system are completed.

CM-3(1) Control Summary Information
Responsible Role:

Parameter CM-3(1):
Parameter CM-3(1)(b):
Parameter CM-3(1)(c):
Parameter CM-3(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-3(1) What is the solution and how is it implemented?

Part a:
Part b:
Part c:
Part d:
Part e:
Part f:

CM-3(2) Testing, Validation, and Documentation of Changes (M)(H)

Test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-3(2) What is the solution and how is it implemented?

CM-3(4) Security and Privacy Representatives (M)(H)

Require [Assignment: organization-defined security and privacy representatives] to be members of the [FedRAMP Assignment: Configuration control board (CCB) or similar (as defined in CM-3)].

CM-3(4) Control Summary Information
Responsible Role:
Parameter CM-3(4)-1:
Parameter CM-3(4)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-3(4) What is the solution and how is it implemented?

CM-3(6) Cryptography Management (H)

Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [FedRAMP Assignment: All security safeguards that rely on cryptography].

CM-3(6) Control Summary Information
Responsible Role:

Parameter CM-3(6):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-3(6) What is the solution and how is it implemented?

CM-4 Impact Analyses (L)(M)(H)

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

CM-4 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CM-4(1) Separate Test Environments (H)

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

CM-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-4(1) What is the solution and how is it implemented?

CM-4(2) Verification of Controls (M)(H)

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

CM-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-4(2) What is the solution and how is it implemented?

CM-5 Access Restrictions for Change (L)(M)(H)

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

CM-5 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-5 What is the solution and how is it implemented?

CM-5(1) Automated Access Enforcement and Audit Records (M)(H)

(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and

(b) Automatically generate audit records of the enforcement actions.

CM-5(1) Control Summary Information
Responsible Role:
Parameter CM-5(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-5(1) What is the solution and how is it implemented?
Part a:
Part b:

CM-5(5) Privilege Limitation for Production and Operation (M)(H)

(a) Limit privileges to change system components and system-related information within a production or operational environment; and

(b) Review and reevaluate privileges [FedRAMP Assignment: at least quarterly].

CM-5(5) Control Summary Information

Responsible Role:
Parameter CM-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-5(5) What is the solution and how is it implemented?
Part a:
Part b:

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

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

CM-6 Additional FedRAMP Requirements and Guidance:

Guidance: Compliance checks are used to evaluate configuration settings and provide general insight into the overall effectiveness of configuration management activities. CSPs and 3PAOs typically combine compliance check findings into a single CM-6 finding, which is acceptable. However, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a per-control basis, where risks exist. Therefore, 3PAOs must also analyze compliance check findings as part of the controls assessment. Where a direct mapping exists, the 3PAO must document additional findings per control in the corresponding SAR Risk Exposure Table (RET), which are then documented in the CSP's Plan of Action and Milestones (POA&M). This will likely result in the details of individual control findings overlapping with those in the combined CM-6 finding, which is acceptable.

During monthly continuous monitoring, new findings from CSP compliance checks may be combined into a single CM-6 POA&M item. CSPs are not required to map the findings to specific controls because controls are only assessed during initial assessments, annual assessments, and significant change requests.

(a) Requirement 1: The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available.

(a) Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).

CM-6 Control Summary Information
Responsible Role:
Parameter CM-6(a):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CM-6(1) Automated Management, Application, and Verification (M)(H)

Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].

CM-6(1) Control Summary Information
Responsible Role:
Parameter CM-6(1)-1:
Parameter CM-6(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-6(1) What is the solution and how is it implemented?

CM-6(2) Respond to Unauthorized Changes (H)

Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].

CM-6(2) Control Summary Information
Responsible Role:
Parameter CM-6(2)-1:
Parameter CM-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-6(2) What is the solution and how is it implemented?

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

a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

CM-7 Additional FedRAMP Requirements and Guidance:

(b) Requirement: The service provider shall use Security guidelines (See CM-6) 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 STIGs or CIS is not available.

CM-7 Control Summary Information
Responsible Role:
Parameter CM-7(a):
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 FedRAMP 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-7(1) Periodic Review (M)(H)

(a) Review the system [FedRAMP Assignment: at least annually] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

(b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].

CM-7(1) Control Summary Information
Responsible Role:
Parameter CM-7(1)(a):
Parameter CM-7(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-7(1) What is the solution and how is it implemented?
Part a:
Part b:

CM-7(2) Prevent Program Execution (M)(H)

Prevent program execution in accordance with [Selection (one-or-more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

CM-7 (2) Additional FedRAMP Requirements and Guidance:

Guidance: This control refers to software deployment by CSP personnel into the production environment. The control requires a policy that states conditions for deploying software. This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e. allow-listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

CM-7(2) Control Summary Information
Responsible Role:
Parameter CM-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-7(2) What is the solution and how is it implemented?

CM-7(5) Authorized Software — Allow-by-exception (M)(H)

(a) Identify [Assignment: organization-defined software programs authorized to execute on the system];

(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

(c) Review and update the list of authorized software programs [FedRAMP Assignment: at least quarterly or when there is a change].

CM-7(5) Control Summary Information
Responsible Role:
Parameter CM-7(5)(a):
Parameter CM-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-7(5) What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Develop and document an inventory of system components that:

   1. Accurately reflects the system;
   2. Includes all components within the system;
   3. Does not include duplicate accounting of components or components assigned to any other system;
   4. Is at the level of granularity deemed necessary for tracking and reporting; and

5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the system component inventory [FedRAMP Assignment: at least monthly].

CM-8 Additional FedRAMP 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)(5):
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 FedRAMP 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-8(1) Updates During Installation and Removal (M)(H)

Update the inventory of system components as part of component installations, removals, and system updates.

CM-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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CM-8(2) Automated Maintenance (H)

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].

CM-8(2) Control Summary Information
Responsible Role:
Parameter CM-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CM-8(3) Automated Unauthorized Component Detection (M)(H)

(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [FedRAMP Assignment: automated mechanisms with a maximum five-minute delay in detection]; and [FedRAMP Assignment: continuously]

(b) Take the following actions when unauthorized components are detected: [Selection (one-or-more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].

CM-8(3) Control Summary Information

Responsible Role:
Parameter CM-8(3)(a)-1:
Parameter CM-8(3)(a)-2:
Parameter CM-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

Part a:
Part b:

CM-8(4) Accountability Information (H)

Include in the system component inventory information, a means for identifying by [FedRAMP Assignment: position and role], individuals responsible and accountable for administering those components.

CM-8(4) Control Summary Information
Responsible Role:
Parameter CM-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CM-9 Configuration Management Plan (M)(H)

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

CM-9 Additional FedRAMP Requirements and Guidance:

Guidance: FedRAMP does not provide a template for the Configuration Management Plan. However, NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, provides guidelines for the implementation of CM controls as well as a sample CMP outline in Appendix D of the Guide.

CM-9 Control Summary Information

Responsible Role:
Parameter CM-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-9 What is the solution and how is it implemented?
Part a:
Part b:

Part c:
Part d:
Part e:

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

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document 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 FedRAMP 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)

a. Establish [Assignment: organization-defined policies] governing the installation of software by users;

b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and

c. Monitor policy compliance [FedRAMP 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 FedRAMP 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:

CM-12 Information Location (M)(H)

a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

CM-12 Additional FedRAMP Requirements and Guidance:

Requirement: According to FedRAMP Authorization Boundary Guidance.

CM-12 Control Summary Information
Responsible Role:
Parameter CM-12(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-12 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

CM-12(1) Automated Tools to Support Information Location (M)(H)

Use automated tools to identify [FedRAMP Assignment: Federal data and system data that must be protected at the High or Moderate impact levels] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.

CM-12 (1) Additional FedRAMP Requirements and Guidance:

Requirement: According to FedRAMP Authorization Boundary Guidance.

CM-12(1) Control Summary Information
Responsible Role:

Parameter CM-12(1)-1:
Parameter CM-12(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-12(1) What is the solution and how is it implemented?

CM-14 Signed Components (H)

Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

CM-14 Additional FedRAMP Requirements and Guidance:

Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized.

CM-14 Control Summary Information
Responsible Role:
Parameter CM-14:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CM-14 What is the solution and how is it implemented?

Contingency Planning

CP-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] contingency planning policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and
2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

CP-1 Control Summary Information
Responsible Role:
Parameter CP-1(a):
Parameter CP-1(a)(1):
Parameter CP-1(b):
Parameter CP-1(c)(1)-1:
Parameter CP-1(c)(1)-2:
Parameter CP-1(c)(2)-1:
Parameter CP-1(c)(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)

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

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

a. Develop a contingency plan for the system that:
    1. Identifies essential mission 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 mission and business functions despite a system disruption, compromise, or failure;
    5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
    6. Addresses the sharing of contingency information; and
    7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [FedRAMP Assignment: at least annually];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

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

Requirement: CSPs must use the FedRAMP Information System Contingency Plan (ISCP) Template (available on the fedramp.gov: https://www.fedramp.gov/assets/resources/templates/SSP-Appendix-G-Information-System-Contingency-Plan-(ISCP)-Template.docx).

CP-2 Control Summary Information
Responsible Role:
Parameter CP-2(a)(7):
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 FedRAMP 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:
Part h:

CP-2(1) Coordinate with Related Plans (M)(H)

Coordinate contingency plan development with organizational elements responsible for related plans.

CP-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CP-2(2) Capacity Planning (H)

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

CP-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-2(2) What is the solution and how is it implemented?

CP-2(3) Resume Mission and Business Functions (M)(H)

Plan for the resumption of [FedRAMP Assignment: all] mission and business functions within [FedRAMP Assignment: time period defined in service provider and organization SLA] of contingency plan activation.

CP-2(3) Control Summary Information
Responsible Role:
Parameter CP-2(3)-1:
Parameter CP-2(3)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-2(3) What is the solution and how is it implemented?

CP-2(5) Continue Mission and Business Functions (H)

Plan for the continuance of [FedRAMP Assignment: essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

CP-2(5) Control Summary Information
Responsible Role:
Parameter CP-2(5):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-2(5) What is the solution and how is it implemented?

CP-2(8) Identify Critical Assets (M)(H)

Identify critical system assets supporting [Selection: Assignment: all; essential] mission and business functions.

CP-2(8) Control Summary Information

Responsible Role:
Parameter CP-2(8):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

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

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

   1. Within [FedRAMP Assignment: *See Additional Requirements] of assuming a contingency role or responsibility;

   2. When required by system changes; and

   3. [FedRAMP Assignment: at least annually] thereafter; and

b. Review and update contingency training content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events].

CP-3 Additional FedRAMP Requirements and Guidance:

(a) Requirement: Privileged admins and engineers must take the basic contingency training within 10 days. Consideration must be given for those privileged admins and engineers with critical contingency-related roles, to gain enough system context and situational awareness to understand the full impact of contingency training as it applies to their respective level. Newly hired critical contingency personnel must take this more in-depth training within 60 days of hire date when the training will have more impact.

CP-3 Control Summary Information
Responsible Role:
Parameter CP-3(a)(1):
Parameter CP-3(a)(3):
Parameter CP-3(b)-1:
Parameter CP-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-3 What is the solution and how is it implemented?
Part a:
Part b:

CP-3(1) Simulated Events (H)

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

CP-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-3(1) What is the solution and how is it implemented?

CP-4 Contingency Plan Testing (L)(M)(H)

a. Test the contingency plan for the system [FedRAMP Assignment: at least annually] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [FedRAMP Assignment: functional exercises].

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

CP-4 Additional FedRAMP Requirements and Guidance:

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

(a) Requirement: The service provider must include the Contingency Plan test results with the security package within the Contingency Plan-designated appendix (Appendix G, Contingency Plan Test Report).

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 FedRAMP 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-4(1) Coordinate with Related Plans (M)(H)

Coordinate contingency plan testing with organizational elements responsible for related plans.

CP-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-4(1) What is the solution and how is it implemented?

CP-4(2) Alternate Processing Site (H)

Test the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

CP-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-4(2) What is the solution and how is it implemented?
Part a:
Part b:

CP-6 Alternate Storage Site (M)(H)

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

CP-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-6 What is the solution and how is it implemented?
Part a:
Part b:

CP-6(1) Separation from Primary Site (M)(H)

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

CP-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-6(1) What is the solution and how is it implemented?

CP-6(2) Recovery Time and Recovery Point Objectives (H)

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

CP-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-6(2) What is the solution and how is it implemented?

CP-6(3) Accessibility (M)(H)

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-6(3) What is the solution and how is it implemented?

CP-7 Alternate Processing Site (M)(H)

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

CP-7 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

CP-7 Control Summary Information
Responsible Role:
Parameter CP-7(a)-1:
Parameter CP-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-7 What is the solution and how is it implemented?

Part a:
Part b:
Part c:

CP-7(1) Separation from Primary Site (M)(H)

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (1) Additional FedRAMP Requirements and Guidance:

Guidance: The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites will be less relevant.

CP-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-7(1) What is the solution and how is it implemented?

CP-7(2) Accessibility (M)(H)

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-7(2) What is the solution and how is it implemented?

CP-7(3) Priority of Service (M)(H)

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

CP-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-7(3) What is the solution and how is it implemented?

CP-7(4) Preparation for Use (H)

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

CP-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-7(4) What is the solution and how is it implemented?

CP-8 Telecommunications Services (M)(H)

Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

CP-8 Control Summary Information
Responsible Role:
Parameter CP-8-1:
Parameter CP-8-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-8 What is the solution and how is it implemented?

CP-8(1) Priority of Service Provisions (M)(H)

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-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) ☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-8(1) What is the solution and how is it implemented?
Part a:
Part b:

CP-8(2) Single Points of Failure (M)(H)

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CP-8(3) Separation of Primary and Alternate Providers (H)

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

CP-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CP-8(4) Provider Contingency Plan (H)

(a) Require primary and alternate telecommunications service providers to have contingency plans;

(b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtain evidence of contingency testing and training by providers [FedRAMP Assignment: annually].

CP-8(4) Control Summary Information
Responsible Role:
Parameter CP-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-8(4) What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Conduct backups of user-level information contained in [Assignment: organization-defined system components]; [FedRAMP Assignment: daily incremental; weekly full]

b. Conduct backups of system-level information contained in the system [FedRAMP Assignment: daily incremental; weekly full];

c. Conduct backups of system documentation, including security- and privacy-related documentation [FedRAMP Assignment: daily incremental; weekly full]; and

d. Protect the confidentiality, integrity, and availability of backup information.

CP-9 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

(a) Requirement: The service provider maintains at least three (3) backup copies of user-level information (at least one (1) of which is available online) or provides an equivalent alternative.

(b) Requirement: The service provider maintains at least three (3) backup copies of system-level information (at least one (1) of which is available online) or provides an equivalent alternative.

(c) Requirement: The service provider maintains at least three (3) backup copies of information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative.

CP-9 Control Summary Information
Responsible Role:
Parameter CP-9(a)-1:

Parameter CP-9(a)-2:
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 FedRAMP 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-9(1) Testing for Reliability and Integrity (M)(H)

Test backup information [FedRAMP Assignment: at least monthly] to verify media reliability and information integrity.

CP-9(1) Control Summary Information
Responsible Role:
Parameter CP-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-9(1) What is the solution and how is it implemented?

CP-9(2) Test Restoration Using Sampling (H)

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

CP-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-9(2) What is the solution and how is it implemented?

CP-9(3) Separate Storage for Critical Information (H)

Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.

CP-9(3) Control Summary Information
Responsible Role:
Parameter CP-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-9(3) What is the solution and how is it implemented?

CP-9(5) Transfer to Alternate Storage Site (H)

Transfer system backup information to the alternate storage site [FedRAMP Assignment: time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA.].

CP-9(5) Control Summary Information
Responsible Role:
Parameter CP-9(5):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-9(5) What is the solution and how is it implemented?

CP-9(8) Cryptographic Protection (M)(H)

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [FedRAMP Assignment: all backup files].

CP-9 (8) Additional FedRAMP Requirements and Guidance:

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

CP-9(8) Control Summary Information
Responsible Role:
Parameter CP-9(8):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-9(8) What is the solution and how is it implemented?

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

Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

CP-10 Control Summary Information
Responsible Role:
Parameter CP-10:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

CP-10(2) Transaction Recovery (M)(H)

Implement transaction recovery for systems that are transaction-based.

CP-10(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-10(2) What is the solution and how is it implemented?

CP-10(4) Restore Within Time Period (H)

Provide the capability to restore system components within [FedRAMP Assignment: time period consistent with the restoration time-periods defined in the service provider and organization SLA] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

CP-10(4) Control Summary Information
Responsible Role:
Parameter CP-10(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-10(4) What is the solution and how is it implemented?

Identification and Authentication

IA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] identification and authentication policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

IA-1 Control Summary Information
Responsible Role:
Parameter IA-1(a):
Parameter IA-1(a)(1):
Parameter IA-1(b):
Parameter IA-1(c)(1)-1:
Parameter IA-1(c)(1)-2:
Parameter IA-1(c)(2)-1:
Parameter IA-1(c)(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)

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

IA-2 Identification and Authentication (Organizational Users) (L)(M)(H)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

IA-2 Additional FedRAMP Requirements and Guidance:

Guidance: "Phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

Requirement: For all control enhancements that specify multifactor authentication, the implementation must adhere to the Digital Identity Guidelines specified in NIST Special Publication 800-63B.

Requirement: Multi-factor authentication must be phishing-resistant.

Requirement: All uses of encrypted virtual private networks must meet all applicable Federal requirements and architecture, dataflow, and security and privacy controls must be documented, assessed, and authorized to operate.

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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

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

Implement multi-factor authentication for access to privileged accounts.

IA-2 (1) Additional FedRAMP Requirements and Guidance:

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

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

Implement multi-factor authentication for access to non-privileged accounts.

IA-2 (2) Additional FedRAMP Requirements and Guidance:

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

IA-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IA-2(5) Individual Authentication with Group Authentication (M)(H)

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

IA-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-2(5) What is the solution and how is it implemented?

IA-2(6) Access to Accounts —separate Device (M)(H)

Implement multi-factor authentication for [FedRAMP Assignment: local, network and remote] access to [FedRAMP Assignment: privileged accounts; non-privileged accounts] such that:

(a) One of the factors is provided by a device separate from the system gaining access; and

(b) The device meets [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography].

IA-2 (6) Additional FedRAMP Requirements and Guidance:

Guidance: PIV=separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials.

Guidance: See SC-13 Guidance for more information on FIPS-validated or NSA-approved cryptography.

IA-2(6) Control Summary Information
Responsible Role:
Parameter IA-2(6)-1:
Parameter IA-2(6)-2:
Parameter IA-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-2(6) What is the solution and how is it implemented?
Part a:
Part b:

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

Implement replay-resistant authentication mechanisms for access to [FedRAMP Assignment: privileged accounts; non-privileged accounts].

IA-2(8) Control Summary Information
Responsible Role:
Parameter IA-2(8):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IA-2(12) Acceptance of PIV Credentials (L)(M)(H)

Accept and electronically verify Personal Identity Verification-compliant credentials.

IA-2 (12) Additional FedRAMP 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IA-3 Device Identification and Authentication (M)(H)

Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one-or-more): local; remote; network] connection.

IA-3 Control Summary Information
Responsible Role:
Parameter IA-3-1:
Parameter IA-3-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-3 What is the solution and how is it implemented?

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

Manage system identifiers by:

a. Receiving authorization from [FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)] to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for [FedRAMP Assignment: at least two (2) years].

IA-4 Control Summary Information
Responsible Role:
Parameter IA-4(a):
Parameter IA-4(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 FedRAMP 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:

IA-4(4) Identify User Status (M)(H)

Manage individual identifiers by uniquely identifying each individual as [FedRAMP Assignment: contractors; foreign nationals].

IA-4(4) Control Summary Information
Responsible Role:

Parameter IA-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

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

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

IA-5 Additional FedRAMP Requirements and Guidance:

Guidance: SP 800-63C Section 6.2.3 Encrypted Assertion requires that authentication assertions be encrypted when passed through third parties, such as a browser. For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE).

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

IA-5 Control Summary Information
Responsible Role:

Parameter IA-5(f)-1:
Parameter IA-5(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 FedRAMP 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:

IA-5(1) Password-based Authentication (L)(M)(H)

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

IA-5 (1) Additional FedRAMP Requirements and Guidance:

Guidance: Note that (c) and (d) require the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13).

Requirement: Password policies must be compliant with NIST SP 800-63B for all memorized, lookup, out-of-band, or One-Time-Passwords (OTP). Password policies shall not enforce special character or minimum password rotation requirements for memorized secrets of users.

(h) Requirement: For cases where technology doesn't allow multi-factor authentication, these rules should be enforced: must have a minimum length of 14 characters and must support all printable ASCII characters.

For emergency use accounts, these rules should be enforced: must have a minimum length of 14 characters, must support all printable ASCII characters, and passwords must be changed if used.

IA-5(1) Control Summary Information
Responsible Role:
Parameter IA-5(1)(a):
Parameter IA-5(1)(h):
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 FedRAMP 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:
Part g:
Part h:

IA-5(2) Public Key-based Authentication (M)(H)

(a) For public key-based authentication:

(1) Enforce authorized access to the corresponding private key; and

(2) Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

(2) Implement a local cache of revocation data to support path discovery and validation.

IA-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-5(2) What is the solution and how is it implemented?
Part a:
Part b:

IA-5(6) Protection of Authenticators (M)(H)

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-5(6) What is the solution and how is it implemented?

IA-5(7) No Embedded Unencrypted Static Authenticators (M)(H)

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

IA-5 (7) Additional FedRAMP Requirements and Guidance:

Guidance: In this context, prohibited static storage refers to any storage where unencrypted authenticators, such as passwords, persist beyond the time required to complete the access process.

IA-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-5(7) What is the solution and how is it implemented?

IA-5(8) Multiple System Accounts (H)

Implement [FedRAMP Assignment: different authenticators in different user authentication domains] to manage the risk of compromise due to individuals having accounts on multiple systems.

IA-5 (8) Additional FedRAMP Requirements and Guidance:

Guidance: If a single user authentication domain is used to access multiple systems, such as in single-sign-on, then only a single authenticator is required.

IA-5(8) Control Summary Information
Responsible Role:
Parameter IA-5(8):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-5(8) What is the solution and how is it implemented?

IA-5(13) Expiration of Cached Authenticators (H)

Prohibit the use of cached authenticators after [Assignment: organization-defined time period].

IA-5 (13) Additional FedRAMP Requirements and Guidance:

Guidance: For components subject to configuration baseline(s) (such as STIG or CIS,) the time period should conform to the baseline standard.

IA-5(13) Control Summary Information
Responsible Role:
Parameter IA-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-5(13) What is the solution and how is it implemented?

IA-6 Authentication Feedback (L)(M)(H)

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

IA-6 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP 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)

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

IA-7 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP 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)

Uniquely identify and authenticate 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IA-8(1) Acceptance of PIV Credentials from Other Agencies (L)(M)(H)

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

IA-8(1) Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented

☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP 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) Acceptance of External Authenticators (L)(M)(H)

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

IA-8(2) Control Summary Information
Responsible Role:

Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-8(2) What is the solution and how is it implemented?
Part a:
Part b:

IA-8(4) Use of Defined Profiles (L)(M)(H)

Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].

IA-8(4) Control Summary Information
Responsible Role:
Parameter IA-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IA-11 Re-authentication (L)(M)(H)

Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

IA-11 Additional FedRAMP Requirements and Guidance:

Guidance: The fixed time period cannot exceed the limits set in SP 800-63. At this time they are:

- AAL3 (high baseline)
  - Twelve (12) hours or
  - Fifteen (15) minutes of inactivity.

IA-11 Control Summary Information
Responsible Role:
Parameter IA-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-11 What is the solution and how is it implemented?

IA-12 Identity Proofing (M)(H)

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

IA-12 Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with NIST SP 800-63A Enrollment and Identity Proofing.

IA-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-12 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

IA-12(2) Identity Evidence (M)(H)

Require evidence of individual identification be presented to the registration authority.

IA-12(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IA-12(3) Identity Evidence Validation and Verification (M)(H)

Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].

IA-12(3) Control Summary Information
Responsible Role:
Parameter IA-12(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-12(3) What is the solution and how is it implemented?

IA-12(4) In-person Validation and Verification (H)

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

IA-12(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-12(4) What is the solution and how is it implemented?

IA-12(5) Address Confirmation (M)(H)

Require that a [Selection: Assignment: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

IA-12 (5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with NIST SP 800-63A Enrollment and Identity Proofing.

IA-12(5) Control Summary Information
Responsible Role:
Parameter IA-12(5):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IA-12(5) What is the solution and how is it implemented?

Incident Response

IR-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] incident response policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and
2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

IR-1 Control Summary Information
Responsible Role:
Parameter IR-1(a):
Parameter IR-1(a)(1):
Parameter IR-1(b):
Parameter IR-1(c)(1)-1:
Parameter IR-1(c)(1)-2:
Parameter IR-1(c)(2)-1:
Parameter IR-1(c)(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)

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

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

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

   1. Within [FedRAMP Assignment: ten (10) days for privileged users, thirty (30) days for Incident Response roles] of assuming an incident response role or responsibility or acquiring system access;

   2. When required by system changes; and

   3. [FedRAMP Assignment: at least annually] thereafter; and

b. Review and update incident response training content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events].

IR-2 Control Summary Information
Responsible Role:
Parameter IR-2(a)(1):
Parameter IR-2(a)(3):

Parameter IR-2(b)-1:
Parameter IR-2(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 FedRAMP 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:

IR-2(1) Simulated Events (H)

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

IR-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IR-2(2) Automated Training Environments (H)

Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].

IR-2(2) Control Summary Information
Responsible Role:
Parameter IR-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-2(2) What is the solution and how is it implemented?

IR-3 Incident Response Testing (M)(H)

Test the effectiveness of the incident response capability for the system [FedRAMP Assignment: at least every six (6) months, including functional at least annually] using the following tests: [Assignment: organization-defined tests].

IR-3-2 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Functional testing must occur prior to testing for initial authorization. Annual functional testing may be concurrent with required penetration tests (see CA-8). The service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to test commencing.

IR-3 Control Summary Information
Responsible Role:
Parameter IR-3-1:
Parameter IR-3-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-3 What is the solution and how is it implemented?

IR-3(2) Coordination with Related Plans (M)(H)

Coordinate incident response testing with organizational elements responsible for related plans.

IR-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-3(2) What is the solution and how is it implemented?

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

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

IR-4 Additional FedRAMP Requirements and Guidance:

Requirement: The FISMA definition of "incident" shall be used: "An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

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 FedRAMP 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:
Part d:

IR-4(1) Automated Incident Handling Processes (M)(H)

Support the incident handling process using [Assignment: organization-defined automated mechanisms].

IR-4(1) Control Summary Information
Responsible Role:
Parameter IR-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-4(1) What is the solution and how is it implemented?

IR-4(2) Dynamic Reconfiguration (H)

Include the following types of dynamic reconfiguration for [FedRAMP Assignment: all network, data storage, and computing devices] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].

IR-4(2) Control Summary Information
Responsible Role:
Parameter IR-4(2)-1:
Parameter IR-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-4(2) What is the solution and how is it implemented?

IR-4(4) Information Correlation (H)

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

IR-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-4(4) What is the solution and how is it implemented?

IR-4(6) Insider Threats (H)

Implement an incident handling capability for incidents involving insider threats.

IR-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-4(6) What is the solution and how is it implemented?

IR-4(11) Integrated Incident Response Team (H)

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].

IR-4(11) Control Summary Information
Responsible Role:
Parameter IR-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-4(11) What is the solution and how is it implemented?

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

Track and document 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IR-5(1) Automated Tracking, Data Collection, and Analysis (H)

Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].

IR-5(1) Control Summary Information
Responsible Role:
Parameter IR-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-5(1) What is the solution and how is it implemented?

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

a. Require personnel to report suspected incidents to the organizational incident response capability within [FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]; and

b. Report incident information to [Assignment: organization-defined authorities].

IR-6 Additional FedRAMP Requirements and Guidance:

Requirement: Reports security incident information according to FedRAMP 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 FedRAMP 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-6(1) Automated Reporting (M)(H)

Report incidents using [Assignment: organization-defined automated mechanisms].

IR-6(1) Control Summary Information

Responsible Role:
Parameter IR-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-6(1) What is the solution and how is it implemented?

IR-6(3) Supply Chain Coordination (M)(H)

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

IR-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-6(3) What is the solution and how is it implemented?

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

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

IR-7(1) Automation Support for Availability of Information and Support (M)(H)

Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].

IR-7(1) Control Summary Information
Responsible Role:
Parameter IR-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-7(1) What is the solution and how is it implemented?

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

a. Develop 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;
8. Addresses the sharing of incident information;

9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [FedRAMP Assignment: at least annually]; and

10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].

b. Distribute copies of the incident response plan to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

IR-8 Additional FedRAMP Requirements and Guidance:

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

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

IR-8 Control Summary Information
Responsible Role:
Parameter IR-8(a)(9)-1:
Parameter IR-8(a)(9)-2:
Parameter IR-8(a)(10):
Parameter IR-8(b):
Parameter IR-8(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 FedRAMP 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:

IR-9 Information Spillage Response (M)(H)

Respond to information spills by:

a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: [Assignment: organization-defined actions].

IR-9 Control Summary Information
Responsible Role:
Parameter IR-9(a):
Parameter IR-9(c):
Parameter IR-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-9 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:
Part f:
Part g:

IR-9(2) Training (M)(H)

Provide information spillage response training [FedRAMP Assignment: at least annually].

IR-9(2) Control Summary Information
Responsible Role:
Parameter IR-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-9(2) What is the solution and how is it implemented?

IR-9(3) Post-spill Operations (M)(H)

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective [Assignment: organization-defined procedures]

IR-9(3) Control Summary Information
Responsible Role:
Parameter IR-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-9(3) What is the solution and how is it implemented?

IR-9(4) Exposure to Unauthorized Personnel (M)(H)

Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].

IR-9(4) Control Summary Information
Responsible Role:
Parameter IR-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

IR-9(4) What is the solution and how is it implemented?

Maintenance

MA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] maintenance policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

MA-1 Control Summary Information
Responsible Role:
Parameter MA-1(a):
Parameter MA-1(a)(1):
Parameter MA-1(b):
Parameter MA-1(c)(1)-1:
Parameter MA-1(c)(1)-2:
Parameter MA-1(c)(2)-1:
Parameter MA-1(c)(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)

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

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

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].

MA-2 Control Summary Information
Responsible Role:
Parameter MA-2(c):
Parameter MA-2(d):
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 FedRAMP 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-2(2) Automated Maintenance Activities (H)

(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; and

(b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

MA-2(2) Control Summary Information
Responsible Role:
Parameter MA-2(2)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-2(2) What is the solution and how is it implemented?
Part a:
Part b:

MA-3 Maintenance Tools (M)(H)

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools [FedRAMP Assignment: at least annually].

MA-3 Control Summary Information

Responsible Role:
Parameter MA-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-3 What is the solution and how is it implemented?
Part a:
Part b:

MA-3(1) Inspect Tools (M)(H)

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

MA-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-3(1) What is the solution and how is it implemented?

MA-3(2) Inspect Media (M)(H)

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

MA-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-3(2) What is the solution and how is it implemented?

MA-3(3) Prevent Unauthorized Removal (M)(H)

Prevent the removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [FedRAMP Assignment: the information owner] explicitly authorizing removal of the equipment from the facility.

MA-3(3) Control Summary Information
Responsible Role:
Parameter MA-3(3)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-3(3) What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

MA-4 Nonlocal Maintenance (L)(M)(H)

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate 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 FedRAMP 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-4(3) Comparable Security and Sanitization (H)

(a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

MA-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-4(3) What is the solution and how is it implemented?
Part a:
Part b:

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

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

MA-5 Control Summary Information
Responsible Role:

Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP 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:

MA-5(1) Individuals Without Appropriate Access (M)(H)

(a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

(1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system.

MA-5(1) Control Summary Information
Responsible Role:
Parameter MA-5(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-5(1) What is the solution and how is it implemented?
Part a:
Part b:

MA-6 Timely Maintenance (M)(H)

Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [FedRAMP Assignment: a timeframe to support advertised uptime and availability] of failure.

MA-6 Control Summary Information
Responsible Role:
Parameter MA-6-1:

Parameter MA-6-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-6 What is the solution and how is it implemented?

Media Protection

MP-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] media protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

   1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

MP-1 Control Summary Information
Responsible Role:
Parameter MP-1(a):
Parameter MP-1(a)(1):

Parameter MP-1(b):
Parameter MP-1(c)(1)-1:
Parameter MP-1(c)(1)-2:
Parameter MP-1(c)(2)-1:
Parameter MP-1(c)(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)

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

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

Restrict access to [FedRAMP Assignment: all types of digital and/or non-digital media containing sensitive information] 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

MP-3 Media Marking (M)(H)

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt [FedRAMP Assignment: no removable media types] from marking if the media remain within [FedRAMP Assignment: organization-defined security safeguards not applicable].

MP-3 Additional FedRAMP Requirements and Guidance:

(b) Guidance: Second parameter not-applicable.

MP-3 Control Summary Information
Responsible Role:
Parameter MP-3(b)-1:
Parameter MP-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MP-3 What is the solution and how is it implemented?
Part a:
Part b:

MP-4 Media Storage (M)(H)

a. Physically control and securely store [FedRAMP Assignment: all types of digital and non-digital media with sensitive information] within [FedRAMP Assignment: see additional FedRAMP requirements and guidance]; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MP-4 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider defines controlled areas within facilities where the information and information system reside.

MP-4 Control Summary Information
Responsible Role:
Parameter MP-4(a)-1:
Parameter MP-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MP-4 What is the solution and how is it implemented?

Part a:
Part b:

MP-5 Media Transport (M)(H)

a. Protect and control [FedRAMP Assignment: all media with sensitive information] during transport outside of controlled areas using [FedRAMP Assignment: prior to leaving secure/controlled environment: for digital media, encryption in compliance with Federal requirements and utilizes FIPS validated or NSA approved cryptography (see SC-13.); for non-digital media, secured in locked container];

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

MP-5 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.

MP-5 Control Summary Information
Responsible Role:
Parameter MP-5(a)-1:
Parameter MP-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

MP-6 Media Sanitization (L)(M)(H)

a. Sanitize [FedRAMP Assignment: techniques and procedures IAW NIST SP 800-88 Section 4: Reuse and Disposal of Storage Media and Hardware] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-6 Control Summary Information
Responsible Role:
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 FedRAMP 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-6(1) Review, Approve, Track, Document, and Verify (H)

Review, approve, track, document, and verify media sanitization and disposal actions.

MP-6 (1) Additional FedRAMP Requirements and Guidance:

Requirement: Must comply with NIST SP 800-88.

MP-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MP-6(1) What is the solution and how is it implemented?

MP-6(2) Equipment Testing (H)

Test sanitization equipment and procedures [FedRAMP Assignment: at least every six (6) months] to ensure that the intended sanitization is being achieved.

MP-6 (2) Additional FedRAMP Requirements and Guidance:

Guidance: Equipment and procedures may be tested or validated for effectiveness.

MP-6(2) Control Summary Information
Responsible Role:
Parameter MP-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MP-6(2) What is the solution and how is it implemented?

MP-6(3) Nondestructive Techniques (H)

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

MP-6 (3) Additional FedRAMP Requirements and Guidance:

Requirement: Must comply with NIST SP 800-88.

MP-6(3) Control Summary Information
Responsible Role:
Parameter MP-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MP-6(3) What is the solution and how is it implemented?

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

a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

MP-7 Control Summary Information
Responsible Role:
Parameter MP-7(a)-1:
Parameter MP-7(a)-2:
Parameter MP-7(a)-3:
Parameter MP-7(a)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

MP-7 What is the solution and how is it implemented?
Part a:
Part b:

Physical and Environmental Protection

PE-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

PE-1 Control Summary Information
Responsible Role:
Parameter PE-1(a):
Parameter PE-1(a)(1):
Parameter PE-1(b):
Parameter PE-1(c)(1)-1:
Parameter PE-1(c)(1)-2:
Parameter PE-1(c)(2)-1:
Parameter PE-1(c)(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)

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

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

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals [FedRAMP Assignment: at least every ninety (90) days]; and

d. Remove 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 FedRAMP 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)

a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using [FedRAMP Assignment: CSP defined physical access control systems/devices AND guards];

b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];

d. Escort visitors and control visitor activity [FedRAMP Assignment: in all circumstances within restricted access area where the information system resides];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [Assignment: organization-defined physical access devices] every [FedRAMP Assignment: at least annually]; and

g. Change combinations and keys [FedRAMP Assignment: at least annually or earlier as required by a security relevant event.] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations 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 FedRAMP 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-3(1) System Access (H)

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].

PE-3(1) Control Summary Information
Responsible Role:
Parameter PE-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-3(1) What is the solution and how is it implemented?

PE-4 Access Control for Transmission (M)(H)

Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].

PE-4 Control Summary Information
Responsible Role:
Parameter PE-4-1:
Parameter PE-4-2:

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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-4 What is the solution and how is it implemented?

PE-5 Access Control for Output Devices (M)(H)

Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.

PE-5 Control Summary Information
Responsible Role:
Parameter PE-5:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-5 What is the solution and how is it implemented?

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

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [FedRAMP Assignment: at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and

c. Coordinate results of reviews and investigations with the organizational 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 FedRAMP 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-6(1) Intrusion Alarms and Surveillance Equipment (M)(H)

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

PE-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-6(1) What is the solution and how is it implemented?

PE-6(4) Monitoring Physical Access to Systems (H)

Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].

PE-6(4) Control Summary Information
Responsible Role:
Parameter PE-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-6(4) What is the solution and how is it implemented?

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

a. Maintain visitor access records to the facility where the system resides for [FedRAMP Assignment: for a minimum of one (1) year];

b. Review visitor access records [FedRAMP Assignment: at least monthly]; and

c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

PE-8 Control Summary Information
Responsible Role:
Parameter PE-8(a):
Parameter PE-8(b):
Parameter PE-8(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 FedRAMP 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:
Part c:

PE-8(1) Automated Records Maintenance and Review (H)

Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].

PE-8(1) Control Summary Information
Responsible Role:
Parameter PE-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

PE-9 Power Equipment and Cabling (M)(H)

Protect power equipment and power cabling for the system from damage and destruction.

PE-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-9 What is the solution and how is it implemented?

PE-10 Emergency Shutoff (M)(H)

a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations;

b. Place emergency shutoff switches or devices in [FedRAMP Assignment: near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off] to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

PE-10 Control Summary Information
Responsible Role:
Parameter PE-10(a):
Parameter PE-10(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-10 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PE-11 Emergency Power (M)(H)

Provide an uninterruptible power supply to facilitate [Selection (one or more): Assignment: an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.

PE-11 Control Summary Information
Responsible Role:
Parameter PE-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-11 What is the solution and how is it implemented?

PE-11(1) Alternate Power Supply — Minimal Operational Capability (H)

Provide an alternate power supply for the system that is activated [FedRAMP Assignment: automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

PE-11(1) Control Summary Information
Responsible Role:
Parameter PE-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-11(1) What is the solution and how is it implemented?

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

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-12 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP 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)

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

PE-13 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable

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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

PE-13(1) Detection Systems — Automatic Activation and Notification (M)(H)

Employ fire detection systems that activate automatically and notify [FedRAMP Assignment: service provider building maintenance/physical security personnel] and [FedRAMP Assignment: service provider emergency responders with incident response responsibilities] in the event of a fire.

PE-13(1) Control Summary Information
Responsible Role:
Parameter PE-13(1)-1:
Parameter PE-13(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-13(1) What is the solution and how is it implemented?

PE-13(2) Suppression Systems — Automatic Activation and Notification (M)(H)

(a) Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

PE-13(2) Control Summary Information
Responsible Role:
Parameter PE-13(2)(a)-1:
Parameter PE-13(2)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-13(2) What is the solution and how is it implemented?
Part a:
Part b:

PE-14 Environmental Controls (L)(M)(H)

a. Maintain [FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and

b. Monitor environmental control levels [FedRAMP Assignment: continuously].

PE-14 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

PE-14 Control Summary Information
Responsible Role:
Parameter PE-14(a)-1:
Parameter PE-14(a)-2:
Parameter PE-14(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 FedRAMP 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-14(2) Monitoring with Alarms and Notifications (H)

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization-defined personnel or roles].

PE-14(2) Control Summary Information
Responsible Role:

Parameter PE-14(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-14(2) What is the solution and how is it implemented?

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

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-15 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

PE-15(1) Automation Support (H)

Detect the presence of water near the system and alert [FedRAMP Assignment: service provider building maintenance/physical security personnel] using [Assignment: organization-defined automated mechanisms].

PE-15(1) Control Summary Information
Responsible Role:
Parameter PE-15(1)-1:
Parameter PE-15(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-15(1) What is the solution and how is it implemented?

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

a. Authorize and control [FedRAMP Assignment: all information system components] entering and exiting the facility; and

b. Maintain records of the system components.

PE-16 Control Summary Information
Responsible Role:
Parameter PE-16(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-16 What is the solution and how is it implemented?
Part a:
Part b:

PE-17 Alternate Work Site (M)(H)

a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;

b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

PE-17 Control Summary Information

Responsible Role:
Parameter PE-17(a):
Parameter PE-17(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-17 What is the solution and how is it implemented?
Part a:

Part b:
Part c:
Part d:

PE-18 Location of System Components (H)

Position system components within the facility to minimize potential damage from [FedRAMP Assignment: physical and environmental hazards identified during threat assessment] and to minimize the opportunity for unauthorized access.

PE-18 Control Summary Information
Responsible Role:
Parameter PE-18:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-18 What is the solution and how is it implemented?

Planning

PL-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] planning policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

PL-1 Control Summary Information
Responsible Role:
Parameter PL-1(a):
Parameter PL-1(a)(1):
Parameter PL-1(b):
Parameter PL-1(c)(1)-1:
Parameter PL-1(c)(1)-2:
Parameter PL-1(c)(2)-1:
Parameter PL-1(c)(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)

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

PL-2 System Security and Privacy Plans (L)(M)(H)

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with [FedRAMP Assignment: to include chief privacy and ISSO and/or similar role or designees]; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [FedRAMP Assignment: to include chief privacy and ISSO and/or similar role];

c. Review the plans [FedRAMP Assignment: at least annually];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

PL-2 Control Summary Information
Responsible Role:
Parameter PL-2(a)(14):
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 FedRAMP 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)(H)

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented 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 system;

c. Review and update the rules of behavior [FedRAMP Assignment: at least annually]; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [FedRAMP Assignment: at least annually and when the rules are revised or changed].

PL-4 Control Summary Information
Responsible Role:
Parameter PL-4(c):
Parameter PL-4(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 FedRAMP 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:

PL-4(1) Social Media and External Site/Application Usage Restrictions (L)(M)(H)

Include in the rules of behavior, restrictions on:

(a) Use of social media, social networking sites, and external sites/applications;

(b) Posting organizational information on public websites; and

(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

PL-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PL-4(1) What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PL-8 Security and Privacy Architectures (L)(M)(H)

a. Develop security and privacy architectures for the system that:

   1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

   2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

   3. Describe how the architectures are integrated into and support the enterprise architecture; and

   4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures [FedRAMP Assignment: at least annually and when a significant change occurs] to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-8 Additional FedRAMP Requirements and Guidance:

(b) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

PL-8 Control Summary Information
Responsible Role:
Parameter PL-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PL-8 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PL-10 Baseline Selection (L)(M)(H)

Select a control baseline for the system.

PL-10 Additional FedRAMP Requirements and Guidance:

Requirement: Select the appropriate FedRAMP Baseline.

PL-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PL-10 What is the solution and how is it implemented?

PL-11 Baseline Tailoring (L)(M)(H)

Tailor the selected control baseline by applying specified tailoring actions.

PL-11 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PL-11 What is the solution and how is it implemented?

Personnel Security

PS-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] personnel security policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

   1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

PS-1 Control Summary Information

Responsible Role:
Parameter PS-1(a):
Parameter PS-1(a)(1):
Parameter PS-1(b):
Parameter PS-1(c)(1)-1:
Parameter PS-1(c)(1)-2:
Parameter PS-1(c)(2)-1:
Parameter PS-1(c)(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)

PS-1 What is the solution and how is it implemented?

Part a:
Part b:
Part c:

PS-2 Position Risk Designation (L)(M)(H)

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [FedRAMP Assignment: at least annually].

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 FedRAMP 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)

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [FedRAMP 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 FedRAMP 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-3(3) Information Requiring Special Protective Measures (M)(H)

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [FedRAMP Assignment: personnel screening criteria – as required by specific information].

PS-3(3) Control Summary Information
Responsible Role:
Parameter PS-3(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PS-3(3) What is the solution and how is it implemented?
Part a:
Part b:

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

Upon termination of individual employment:

a. Disable system access within [FedRAMP Assignment: one (1) hour];

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-4 Control Summary Information
Responsible Role:
Parameter PS-4(a):
Parameter PS-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 FedRAMP 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:

PS-4(2) Automated Actions (H)

Use [Assignment: organization-defined automated mechanisms] to [Selection (one-or-more): notify [FedRAMP Assignment: access control personnel responsible for disabling access to the system] of individual termination actions; disable access to system resources].

PS-4(2) Control Summary Information
Responsible Role:
Parameter PS-4(2)-1:
Parameter PS-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PS-4(2) What is the solution and how is it implemented?

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

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [FedRAMP Assignment: twenty-four (24) hours];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [FedRAMP Assignment: including access control personnel responsible for the system] within [FedRAMP Assignment: twenty-four (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 FedRAMP 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)(H)

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements [FedRAMP Assignment: at least annually]; and

c. Verify that individuals requiring access to organizational information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [FedRAMP Assignment: at least annually and any time there is a change to the user's level of access].

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 FedRAMP 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 External Personnel Security (L)(M)(H)

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify [FedRAMP Assignment: including access control personnel responsible for the system and/or facilities, as appropriate] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [FedRAMP Assignment: terminations: immediately; transfers: within twenty-four (24) hours]; and

e. Monitor provider compliance with personnel security requirements.

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 FedRAMP 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)(H)

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify [FedRAMP Assignment: to include the ISSO and/or similar role within the organization] within [FedRAMP Assignment: Twenty-four (24) hours] 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 FedRAMP 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:

PS-9 Position Descriptions (L)(M)(H)

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

PS-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

PS-9 What is the solution and how is it implemented?

Risk Assessment

RA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] risk assessment policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

RA-1 Control Summary Information
Responsible Role:
Parameter RA-1(a):
Parameter RA-1(a)(1):
Parameter RA-1(b):
Parameter RA-1(c)(1)-1:
Parameter RA-1(c)(1)-2:
Parameter RA-1(c)(2)-1:
Parameter RA-1(c)(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)

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

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

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-2 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP 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)(H)

a. Conduct a risk assessment, including:

   1. Identifying threats to and vulnerabilities in the system;

   2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

   3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [FedRAMP Assignment: security assessment report];

d. Review risk assessment results [FedRAMP Assignment: at least annually and whenever a significant change occurs];

e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and

f. Update the risk assessment [FedRAMP Assignment: annually] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

(e) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-3 Control Summary Information
Responsible Role:
Parameter RA-3(c):
Parameter RA-3(d):
Parameter RA-3(e):
Parameter RA-3(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 FedRAMP 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:
Part f:

RA-3(1) Supply Chain Risk Assessment (L)(M)(H)

(a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and

(b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in supply chain.

RA-3(1) Control Summary Information
Responsible Role:
Parameter RA-3(1)(a):
Parameter RA-3(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-3(1) What is the solution and how is it implemented?
Part a:
Part b:

RA-5 Vulnerability Monitoring and Scanning (L)(M)(H)

a. Monitor and scan for vulnerabilities in the system and hosted applications [FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications (including APIs) and databases] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

   1. Enumerating platforms, software flaws, and improper configurations;

   2. Formatting checklists and test procedures; and

   3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities [FedRAMP 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;

e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5 Additional FedRAMP Requirements and Guidance:

Guidance: See the FedRAMP Documents page > Vulnerability Scanning Requirements https://www.FedRAMP.gov/documents/

Guidance: Informational findings from a scanner are detailed as a returned result that holds no vulnerability risk or severity, and for FedRAMP, does not require an entry onto the POA&M or entry onto the RET during any assessment phase.

Warning findings, on the other hand, are given a risk rating (low, moderate, high or critical) by the scanning solution and should be treated like any other finding with a risk or severity rating for tracking purposes onto either the POA&M or RET depending on when the findings originated (during assessments or during monthly continuous monitoring). If a warning is received during scanning, but further validation turns up no actual issue then this item should be categorized as a false positive. If this situation presents itself during an assessment phase (initial assessment, annual assessment or

any SCR), follow guidance on how to report false positives in the Security Assessment Report (SAR). If this situation happens during monthly continuous monitoring, a deviation request will need to be submitted per the FedRAMP Vulnerability Deviation Request Form.

Warnings are commonly associated with scanning solutions that also perform compliance scans, and if the scanner reports a "warning" as part of the compliance scanning of a CSO, follow guidance surrounding the tracking of compliance findings during either the assessment phases (initial assessment, annual assessment or any SCR) or monthly continuous monitoring as it applies. Guidance on compliance scan findings can be found by searching on "Tracking of Compliance Scans" in FAQs.

(a) Requirement: an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

(d) Requirement: If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) the KEV remediation date supersedes the FedRAMP parameter requirement.

(e) Requirement: to include all Authorizing Officials; for JAB authorizations to include FedRAMP.

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 FedRAMP 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:
Part f:

RA-5(2) Update Vulnerabilities to Be Scanned (L)(M)(H)

Update the system vulnerabilities to be scanned [FedRAMP Assignment: within twenty-four (24) hours prior to running scans].

RA-5(2) Control Summary Information
Responsible Role:
Parameter RA-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-5(2) What is the solution and how is it implemented?

RA-5(3) Breadth and Depth of Coverage (M)(H)

Define the breadth and depth of vulnerability scanning coverage.

RA-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-5(3) What is the solution and how is it implemented?

RA-5(4) Discoverable Information (H)

Determine information about the system that is discoverable and take [FedRAMP Assignment: notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions].

RA-5(4) Control Summary Information
Responsible Role:
Parameter RA-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-5(4) What is the solution and how is it implemented?

RA-5(5) Privileged Access (M)(H)

Implement privileged access authorization to [FedRAMP Assignment: all components that support authentication] for [FedRAMP Assignment: all scans].

RA-5(5) Control Summary Information
Responsible Role:
Parameter RA-5(5)-1:
Parameter RA-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-5(5) What is the solution and how is it implemented?

RA-5(8) Review Historic Audit Logs (H)

Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

RA-5(8) Additional FedRAMP Requirement:

Requirement: This enhancement is required for all high (or critical) vulnerability scan findings.

RA-5(8) Control Summary Information
Responsible Role:
Parameter RA-5(8)-1:

Parameter RA-5(8)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-5(8) What is the solution and how is it implemented?

RA-5(11) Public Disclosure Program (L)(M)(H)

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA-5(11) Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

RA-7 Risk Response (L)(M)(H)

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA-7 Control Summary Information
Responsible Role:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-7 What is the solution and how is it implemented?

RA-9 Criticality Analysis (M)(H)

Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].

RA-9 Control Summary Information
Responsible Role:
Parameter RA-9-1:
Parameter RA-9-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

RA-9 What is the solution and how is it implemented?

System and Services Acquisition

SA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and services acquisition policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SA-1 Control Summary Information
Responsible Role:
Parameter SA-1(a):
Parameter SA-1(a)(1):
Parameter SA-1(b):
Parameter SA-1(c)(1)-1:
Parameter SA-1(c)(1)-2:
Parameter SA-1(c)(2)-1:
Parameter SA-1(c)(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)

SA-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SA-2 Allocation of Resources (L)(M)(H)

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy 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 FedRAMP 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)

a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy 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 FedRAMP 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 Acquisition Process (L)(M)(H)

Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one-or-more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

SA-4 Additional FedRAMP Requirements and Guidance:

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.

See https://www.niap-ccevs.org/Product/index.cfm or https://www.commoncriteriaportal.org/products/.

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).

SA-4 Control Summary Information
Responsible Role:
Parameter SA-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 FedRAMP 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:
Part h:
Part i:

SA-4(1) Functional Properties of Controls (M)(H)

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

SA-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-4(1) What is the solution and how is it implemented?

SA-4(2) Design and Implementation Information for Controls (M)(H)

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [FedRAMP Assignment: at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram; organization-defined design/implementation information] at [Assignment: organization-defined level of detail].

SA-4(2) Control Summary Information
Responsible Role:
Parameter SA-4(2)-1:
Parameter SA-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-4(2) What is the solution and how is it implemented?

SA-4(5) System, Component, and Service Configurations (H)

Require the developer of the system, system component, or system service to:

(a) Deliver the system, component, or service with [FedRAMP Assignment: The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available.] implemented; and

(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

SA-4(5) Control Summary Information
Responsible Role:
Parameter SA-4(5)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-4(5) What is the solution and how is it implemented?
Part a:
Part b:

SA-4(9) Functions, Ports, Protocols, and Services in Use (M)(H)

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

SA-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-4(9) What is the solution and how is it implemented?

SA-4(10) Use of Approved PIV Products (L)(M)(H)

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

SA-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-4(10) What is the solution and how is it implemented?

SA-5 System Documentation (L)(M)(H)

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;

   2. Effective use and maintenance of security and privacy functions and mechanisms; and

   3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

   1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

   3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and

d. Distribute documentation to [FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)].

SA-5 Control Summary Information
Responsible Role:
Parameter SA-5(c):
Parameter SA-5(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 FedRAMP 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:

SA-8 Security and Privacy Engineering Principles (L)(M)(H)

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].

SA-8 Control Summary Information
Responsible Role:

Parameter SA-8:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-8 What is the solution and how is it implemented?

SA-9 External System Services (L)(M)(H)

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [FedRAMP Assignment: Appropriate FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system];

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored].

SA-9 Control Summary Information
Responsible Role:
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 FedRAMP 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:

SA-9(1) Risk Assessments and Organizational Approvals (M)(H)

(a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

(b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

SA-9(1) Control Summary Information
Responsible Role:
Parameter SA-9(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-9(1) What is the solution and how is it implemented?
Part a:
Part b:

SA-9(2) Identification of Functions, Ports, Protocols, and Services (M)(H)

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [FedRAMP Assignment: all external systems where Federal information is processed or stored].

SA-9(2) Control Summary Information
Responsible Role:
Parameter SA-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-9(2) What is the solution and how is it implemented?

SA-9(5) Processing, Storage, and Service Location (M)(H)

Restrict the location of [FedRAMP Assignment: information processing, information or data, AND system services] to [FedRAMP Assignment: U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction] based on [FedRAMP Assignment: all High impact data, systems, or services].

SA-9(5) Control Summary Information
Responsible Role:
Parameter SA-9(5)-1:
Parameter SA-9(5)-2:
Parameter SA-9(5)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-9(5) What is the solution and how is it implemented?

SA-10 Developer Configuration Management (M)(H)

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service [FedRAMP Assignment: development, implementation, AND operation];

b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

SA-10 Additional FedRAMP Requirements and Guidance:

(e) Requirement: track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.

SA-10 Control Summary Information
Responsible Role:

Parameter SA-10(a):
Parameter SA-10(b):
Parameter SA-10(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-10 What is the solution and how is it implemented?
Part a:

Part b:
Part c:
Part d:
Part e:

SA-11 Developer Testing and Evaluation (M)(H)

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy assessments;

b. Perform [Selection (one-or-more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

SA-11 Control Summary Information
Responsible Role:
Parameter SA-11(b)-1:
Parameter SA-11(b)-2:
Parameter SA-11(b)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-11 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:

SA-11(1) Static Code Analysis (M)(H)

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11(1) Additional FedRAMP Requirements:

Requirement: The service provider must document its methodology for reviewing newly developed code for the Service in its Continuous Monitoring Plan.

If Static code analysis cannot be performed (for example, when the source code is not available), then dynamic code analysis must be performed (see SA-11 (8)).

SA-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-11(1) What is the solution and how is it implemented?

SA-11(2) Threat Modeling and Vulnerability Analyses (M)(H)

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

(a) Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];

(b) Employs the following tools and methods: [Assignment: organization-defined tools and methods];

(c) Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and

(d) Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].

SA-11(2) Control Summary Information
Responsible Role:
Parameter SA-11(2)(a):
Parameter SA-11(2)(b):
Parameter SA-11(2)(c):

Parameter SA-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-11(2) What is the solution and how is it implemented?
Part a:
Part b:
Part c:

Part d:

SA-15 Development Process, Standards, and Tools (M)(H)

a. Require the developer of the system, system component, or system service to follow a documented development process that:

   1. Explicitly addresses security and privacy requirements;

   2. Identifies the standards and tools used in the development process;

   3. Documents the specific tool options and tool configurations used in the development process; and

   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations [FedRAMP Assignment: frequency as before first use and annually thereafter] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [FedRAMP Assignment: FedRAMP Security Authorization requirements].

SA-15 Control Summary Information
Responsible Role:
Parameter SA-15(b)-1:
Parameter SA-15(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-15 What is the solution and how is it implemented?
Part a:
Part b:

SA-15(3) Criticality Analysis (M)(H)

Require the developer of the system, system component, or system service to perform a criticality analysis:

(a) At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; and

(b) At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis].

SA-15(3) Control Summary Information
Responsible Role:
Parameter SA-15(3)(a):
Parameter SA-15(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-15(3) What is the solution and how is it implemented?

Part a:
Part b:

SA-16 Developer-provided Training (H)

Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].

SA-16 Control Summary Information
Responsible Role:
Parameter SA-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-16 What is the solution and how is it implemented?

SA-17 Developer Security and Privacy Architecture and Design (H)

Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;

b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and

c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

SA-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-17 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SA-21 Developer Screening (H)

Require that the developer of [Assignment: organization-defined system, system component, or system service]:

a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and

b. Satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria].

SA-21 Control Summary Information
Responsible Role:
Parameter SA-21:
Parameter SA-21(a):
Parameter SA-21(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-21 What is the solution and how is it implemented?
Part a:
Part b:

SA-22 Unsupported System Components (L)(M)(H)

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one-or-more): in-house support; [Assignment: organization-defined support from external providers]].

SA-22 Control Summary Information
Responsible Role:
Parameter SA-22(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SA-22 What is the solution and how is it implemented?
Part a:
Part b:

System and Communications Protection

SC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and communications protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SC-1 Control Summary Information
Responsible Role:
Parameter SC-1(a):
Parameter SC-1(a)(1):
Parameter SC-1(b):
Parameter SC-1(c)(1)-1:
Parameter SC-1(c)(1)-2:
Parameter SC-1(c)(2)-1:

Parameter SC-1(c)(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)

SC-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SC-2 Separation of System and User Functionality (M)(H)

Separate user functionality, including user interface services, from system management functionality.

SC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-2 What is the solution and how is it implemented?

SC-3 Security Function Isolation (H)

Isolate security functions from nonsecurity functions.

SC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-3 What is the solution and how is it implemented?

SC-4 Information in Shared System Resources (M)(H)

Prevent unauthorized and unintended information transfer via shared system resources.

SC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-4 What is the solution and how is it implemented?

SC-5 Denial-of-service Protection (L)(M)(H)

a. [FedRAMP Assignment: Protect against] the effects of the following types of denial-of-service events: [FedRAMP Assignment: at a minimum: ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack] and;

b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].

SC-5 Control Summary Information
Responsible Role:
Parameter SC-5(a)-1:
Parameter SC-5(a)-2:
Parameter SC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-5 What is the solution and how is it implemented?
Part a:
Part b:

SC-7 Boundary Protection (L)(M)(H)

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces with

b. Implement subnetworks for publicly accessible system components that are [Assignment: physically; logically] separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

SC-7 Additional FedRAMP Requirements and Guidance:

(b) Guidance: SC-7 (b) should be met by subnet isolation. A subnetwork (subnet) is a physically or logically segmented section of a larger network defined at TCP/IP Layer 3, to both minimize traffic and, important for a FedRAMP Authorization, add a crucial layer of network isolation. Subnets are distinct from VLANs (Layer 2), security groups, and VPCs and are specifically required to satisfy SC-7 part b and other controls.

See the FedRAMP Subnets White Paper (https://www.fedramp.gov/assets/resources/documents/FedRAMP_subnets_white_paper.pdf) for additional information.

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 FedRAMP 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-7(3) Access Points (M)(H)

Limit the number of external network connections to the system.

SC-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(3) What is the solution and how is it implemented?

SC-7(4) External Telecommunications Services (M)(H)

(a) Implement a managed interface for each external telecommunication service;

(b) Establish a traffic flow policy for each managed interface;

(c) Protect the confidentiality and integrity of the information being transmitted across each interface;

(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

(e) Review exceptions to the traffic flow policy [FedRAMP Assignment: at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions] and remove exceptions that are no longer supported by an explicit mission or business need;

(f) Prevent unauthorized exchange of control plane traffic with external networks;

(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

(h) Filter unauthorized control plane traffic from external networks.

SC-7(4) Control Summary Information
Responsible Role:

Parameter SC-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(4) 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:

SC-7(5) Deny by Default — Allow by Exception (M)(H)

Deny network communications traffic by default and allow network communications traffic by exception [Selection (one-or-more): at managed interfaces; for [FedRAMP Assignment: any systems].

SC-7 (5) Additional FedRAMP Requirements and Guidance:

Guidance: For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing

SC-7(5) Control Summary Information
Responsible Role:
Parameter SC-7(5):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(5) What is the solution and how is it implemented?

SC-7(7) Split Tunneling for Remote Devices (M)(H)

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].

SC-7(7) Control Summary Information
Responsible Role:
Parameter SC-7(7):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(7) What is the solution and how is it implemented?

SC-7(8) Route Traffic to Authenticated Proxy Servers (M)(H)

Route [Assignment: organization-defined internal communications traffic] to [FedRAMP Assignment: any network outside of organizational control and any network outside the authorization boundary] through authenticated proxy servers at managed interfaces.

SC-7(8) Control Summary Information
Responsible Role:

Parameter SC-7(8)-1:
Parameter SC-7(8)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(8) What is the solution and how is it implemented?

SC-7(10) Prevent Exfiltration (H)

(a) Prevent the exfiltration of information; and

(b) Conduct exfiltration tests [Assignment: organization-defined frequency].

SC-7(10) Control Summary Information
Responsible Role:
Parameter SC-7(10)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(10) What is the solution and how is it implemented?
Part a:
Part b:

SC-7(12) Host-based Protection (M)(H)

Implement [FedRAMP Assignment: Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall] at [Assignment: organization-defined system components].

SC-7(12) Control Summary Information
Responsible Role:
Parameter SC-7(12)-1:
Parameter SC-7(12)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(12) What is the solution and how is it implemented?

SC-7(18) Fail Secure (M)(H)

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

SC-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(18) What is the solution and how is it implemented?

SC-7(20) Dynamic Isolation and Segregation (H)

Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.

SC-7(20) Control Summary Information
Responsible Role:
Parameter SC-7(20):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(20) What is the solution and how is it implemented?

SC-7(21) Isolation of System Components (H)

Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].

SC-7(21) Control Summary Information
Responsible Role:
Parameter SC-7(21)-1:
Parameter SC-7(21)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-7(21) What is the solution and how is it implemented?

SC-8 Transmission Confidentiality and Integrity (L)(M)(H)

Protect the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

SC-8 Additional FedRAMP Requirements and Guidance:

Guidance: For each instance of data in transit, confidentiality AND integrity should be through cryptography as specified in SC-8 (1), physical means as specified in SC-8 (5), or in combination.

For clarity, this control applies to all data in transit. Examples include the following data flows:

- Crossing the system boundary
- Between compute instances - including containers
- From a compute instance to storage
- Replication between availability zones
- Transmission of backups to storage
- From a load balancer to a compute instance
- Flows from management tools required for their work – e.g. log collection, scanning, etc.

The following applies only when choosing SC-8 (5) in lieu of SC-8 (1).

FedRAMP-Defined Assignment / Selection Parameters

SC-8 (5)-1 [a hardened or alarmed carrier Protective Distribution System (PDS) when outside of Controlled Access Area (CAA)]

SC-8 (5)-2 [prevent unauthorized disclosure of information AND detect changes to information]

Guidance: SC-8 (5) applies when physical protection has been selected as the method to protect confidentiality and integrity. For physical protection, data in transit must be in either a Controlled Access Area (CAA), or a Hardened or alarmed PDS.

Hardened or alarmed PDS: Shall be as defined in SECTION X - CATEGORY 2 PDS INSTALLATION GUIDANCE of CNSSI No.7003, titled PROTECTED DISTRIBUTION SYSTEMS (PDS). Per the CNSSI No. 7003 Section VIII, PDS must originate and terminate in a Controlled Access Area (CAA).

Controlled Access Area (CAA): Data will be considered physically protected, and in a CAA if it meets Section 2.3 of the DHS's Recommended Practice: Improving Industrial

Control System Cybersecurity with Defense-in-Depth Strategies. CSPs can meet Section 2.3 of the DHS' recommended practice by satisfactory implementation of the following controls PE-2 (1), PE-2 (2), PE-2 (3), PE-3 (2), PE-3 (3), PE-6 (2), and PE-6 (3). Note: When selecting SC-8 (5), the above SC-8(5), and the above referenced PE controls must be added to the SSP. CNSSI No.7003 can be accessed here: https://www.dcsa.mil/Portals/91/documents/ctp/nao/CNSSI_7003_PDS_September_2015.pdf DHS Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies can be accessed here: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf.

SC-8 Control Summary Information
Responsible Role:
Parameter SC-8:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-8 What is the solution and how is it implemented?

SC-8(1) Cryptographic Protection (L)(M)(H)

Implement cryptographic mechanisms to [FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information] during transmission.

SC-8 (1) Additional FedRAMP Requirements and Guidance:

Guidance: See M-22-09, including "Agencies encrypt all DNS requests and HTTP traffic within their environment" SC-8 (1) applies when encryption has been selected as the method to protect confidentiality and integrity. Otherwise refer to SC-8 (5). SC-8 (1) is strongly encouraged.

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

Guidance: When leveraging encryption from the underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Requirement: Please ensure SSP Section 10.3 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT) is fully populated for reference in this control.

SC-8(1) Control Summary Information

Responsible Role:
Parameter SC-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

SC-10 Network Disconnect (M)(H)

Terminate the network connection associated with a communications session at the end of the session or after [FedRAMP Assignment: no longer than ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for user sessions] of inactivity.

SC-10 Control Summary Information
Responsible Role:
Parameter SC-10:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-10 What is the solution and how is it implemented?

SC-12 Cryptographic Key Establishment and Management (L)(M)(H)

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [FedRAMP Assignment: In accordance with Federal requirements].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: See references in NIST 800-53 documentation.

Guidance: Must meet applicable Federal Cryptographic Requirements. See References Section of control.

Guidance: Wildcard certificates may be used internally within the system, but are not permitted for external customer access to the system.

SC-12 Control Summary Information
Responsible Role:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-12 What is the solution and how is it implemented?

SC-12(1) Availability (H)

Maintain availability of information in the event of the loss of cryptographic keys by users.

SC-12(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-12(1) What is the solution and how is it implemented?

SC-13 Cryptographic Protection (L)(M)(H)

a. Determine the [Assignment: organization-defined cryptographic uses]; and

b. Implement the following types of cryptography required for each specified cryptographic use: [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography].

SC-13 Additional FedRAMP Requirements and Guidance:

Guidance: This control applies to all use of cryptography. In addition to encryption, this includes functions such as hashing, random number generation, and key generation. Examples include the following:

- Encryption of data
- Decryption of data
- Generation of one time passwords (OTPs) for MFA
- Protocols such as TLS, SSH, and HTTPS

The requirement for FIPS 140 validation, as well as timelines for acceptance of FIPS 140-2, and 140-3 can be found at the NIST Cryptographic Module Validation Program (CMVP). https://csrc.nist.gov/projects/cryptographic-module-validation-program.

Guidance: For NSA-approved cryptography, the National Information Assurance Partnership (NIAP) oversees a national program to evaluate Commercial IT Products for Use in National Security Systems. The NIAP Product Compliant List can be found at the following location: https://www.niap-ccevs.org/Product/index.cfm.

Guidance: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Guidance: Moving to non-FIPS CM or product is acceptable when:

- FIPS validated version has a known vulnerability
- Feature with vulnerability is in use
- Non-FIPS version fixes the vulnerability
- Non-FIPS version is submitted to NIST for FIPS validation
- POA&M is added to track approval, and deployment when ready

Guidance: At a minimum, this control applies to cryptography in use for the following controls: AU-9(3), CP-9(8), IA-2(6), IA-5(1), MP-5, SC-8(1), and SC-28(1).

SC-13 Control Summary Information

Responsible Role:
Parameter SC-13(a):
Parameter SC-13(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-13 What is the solution and how is it implemented?
Part a:

Part b:

SC-15 Collaborative Computing Devices and Applications (L)(M)(H)

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [FedRAMP Assignment: no exceptions for computing devices]; and

b. Provide an explicit indication of use to users physically present at the devices.

SC-15 Additional FedRAMP 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 FedRAMP 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-17 Public Key Infrastructure Certificates (M)(H)

a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

SC-17 Control Summary Information
Responsible Role:
Parameter SC-17(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-17 What is the solution and how is it implemented?
Part a:
Part b:

SC-18 Mobile Code (M)(H)

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

SC-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-18 What is the solution and how is it implemented?
Part a:
Part b:

SC-20 Secure Name/Address Resolution Service (Authoritative Source) (L)(M)(H)

a. Provide 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

b. Provide 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 Additional FedRAMP Requirements and Guidance:

Guidance: SC-20 applies to use of external authoritative DNS to access a CSO from outside the boundary.

Guidance: External authoritative DNS servers may be located outside an authorized environment. Positioning these servers inside an authorized boundary is encouraged.

Guidance: CSPs are recommended to self-check DNSSEC configuration through one of many available analyzers such as Sandia National Labs (https://dnsviz.net)

Requirement: Control Description should include how DNSSEC is implemented on authoritative DNS servers to supply valid responses to external DNSSEC requests.

Requirement: Authoritative DNS servers must be geolocated in accordance with SA-9 (5).

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 FedRAMP 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)

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-21 Additional FedRAMP Requirements and Guidance:

Guidance: Accepting an unsigned reply is acceptable

Guidance: SC-21 applies to use of internal recursive DNS to access a domain outside the boundary by a component inside the boundary. DNSSEC resolution to access a component inside the boundary is excluded.

Requirement: Control description should include how DNSSEC is implemented on recursive DNS servers to make DNSSEC requests when resolving DNS requests from internal components to domains external to the CSO boundary.

- If the reply is signed, and fails DNSSEC, do not use the reply
- If the reply is unsigned:
    - CSP chooses the policy to apply.

Requirement: Internal recursive DNS servers must be located inside an authorized environment. It is typically within the boundary, or leveraged from an underlying IaaS/PaaS.

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 FedRAMP 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)

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-22 What is the solution and how is it implemented?

SC-23 Session Authenticity (M)(H)

Protect the authenticity of communications sessions.

SC-23 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-23 What is the solution and how is it implemented?

SC-24 Fail in Known State (H)

Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [list of organization-defined types of system failures on organization-defined system components].

SC-24 Control Summary Information
Responsible Role:

Parameter SC-24-1:
Parameter SC-24-2:
Parameter SC-24-3:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-24 What is the solution and how is it implemented?

SC-28 Protection of Information at Rest (L)(M)(H)

Protect the [FedRAMP Assignment: confidentiality AND integrity] of the following information at rest: [Assignment: organization-defined information at rest].

SC-28 Additional FedRAMP Requirements and Guidance:

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

Guidance: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Guidance: Note that this enhancement requires the use of cryptography in accordance with SC-13.

SC-28 Control Summary Information
Responsible Role:
Parameter SC-28-1:
Parameter SC-28-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-28 What is the solution and how is it implemented?

SC-28(1) Cryptographic Protection (L)(M)(H)

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [FedRAMP Assignment: all information system components storing Federal data or system data that must be protected at the High or Moderate impact levels]: [Assignment: organization-defined information].

SC-28 (1) Additional FedRAMP Requirements and Guidance:

Guidance: Organizations should select a mode of protection that is targeted towards the relevant threat scenarios.

Examples:

A. Organizations may apply full disk encryption (FDE) to a mobile device where the primary threat is loss of the device while storage is locked.

B. For a database application housing data for a single customer, encryption at the file system level would often provide more protection than FDE against the more likely threat of an intruder on the operating system accessing the storage.

C. For a database application housing data for multiple customers, encryption with unique keys for each customer at the database record level may be more appropriate.

SC-28(1) Control Summary Information
Responsible Role:
Parameter SC-28(1)-1:
Parameter SC-28(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-28(1) What is the solution and how is it implemented?

SC-39 Process Isolation (L)(M)(H)

Maintain a separate execution domain for each executing system 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-39 What is the solution and how is it implemented?

SC-45 System Time Synchronization (M)(H)

Synchronize system clocks within and between systems and system components.

SC-45 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-45 What is the solution and how is it implemented?

SC-45(1) Synchronization with Authoritative Time Source (M)(H)

(a) Compare the internal system clocks [FedRAMP Assignment: At least hourly] with [FedRAMP Assignment: http://tf.nist.gov/tf-cgi/servers.cgi]; and

(b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [FedRAMP Assignment: any difference].

SC-45(1) Additional FedRAMP Requirements and Guidance:

Guidance: Synchronization of system clocks improves the accuracy of log analysis.

Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

SC-45(1) Control Summary Information
Responsible Role:

Parameter SC-45(1)(a)-1:
Parameter SC-45(1)(a)-2:
Parameter SC-45(1)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SC-45(1) What is the solution and how is it implemented?
Part a:

Part b:

System and Information Integrity

SI-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and information integrity policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

   1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SI-1 Control Summary Information

Responsible Role:
Parameter SI-1(a):
Parameter SI-1(a)(1):
Parameter SI-1(b):
Parameter SI-1(c)(1)-1:
Parameter SI-1(c)(1)-2:
Parameter SI-1(c)(2)-1:
Parameter SI-1(c)(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)

SI-1 What is the solution and how is it implemented?

Part a:
Part b:
Part c:

SI-2 Flaw Remediation (L)(M)(H)

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [FedRAMP Assignment: within thirty (30) days of release of updates] of the release of the updates; and

d. Incorporate 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 FedRAMP 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-2(2) Automated Flaw Remediation Status (M)(H)

Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms].[FedRAMP Assignment: at least monthly]

SI-2(2) Control Summary Information
Responsible Role:
Parameter SI-2(2)-1:

Parameter SI-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-2(2) What is the solution and how is it implemented?

SI-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions (M)(H)

(a) Measure the time between flaw identification and flaw remediation; and

(b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].

SI-2(3) Control Summary Information
Responsible Role:
Parameter SI-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-2(3) What is the solution and how is it implemented?

Part a:
Part b:

SI-3 Malicious Code Protection (L)(M)(H)

a. Implement [FedRAMP Assignment: signature based and non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

   1. Perform periodic scans of the system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints and network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

   2. [FedRAMP Assignment: [to include blocking and quarantining malicious code]; and send alert to [FedRAMP Assignment: [administrator or defined security personnel near-real time] in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-3 Control Summary Information
Responsible Role:
Parameter SI-3(a):
Parameter SI-3(c)(1)-1:

Parameter SI-3(c)(1)-2:
Parameter SI-3(c)(2)-1:
Parameter SI-3(c)(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 FedRAMP 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 System Monitoring (L)(M)(H)

a. Monitor the system to detect:

   1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and

   2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

   1. Strategically within the system to collect organization-determined essential information; and

   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one-or-more): as needed; [Assignment: organization-defined frequency]].

SI-4 Additional FedRAMP 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 FedRAMP 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-4(1) System-wide Intrusion Detection System (M)(H)

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

SI-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(1) What is the solution and how is it implemented?

SI-4(2) Automated Tools and Mechanisms for Real-time Analysis (M)(H)

Employ automated tools and mechanisms to support near real-time analysis of events.

SI-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(2) What is the solution and how is it implemented?

SI-4(4) Inbound and Outbound Communications Traffic (M)(H)

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic [FedRAMP Assignment: continuously] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

SI-4(4) Control Summary Information
Responsible Role:
Parameter SI-4(4)(b)-1:
Parameter SI-4(4)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(4) What is the solution and how is it implemented?

Part a:
Part b:

SI-4(5) System-generated Alerts (M)(H)

Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

SI-4 (5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with the incident response plan.

SI-4(5) Control Summary Information
Responsible Role:
Parameter SI-4(5)-1:
Parameter SI-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(5) What is the solution and how is it implemented?

SI-4(10) Visibility of Encrypted Communications (H)

Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].

SI-4 (10) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).

SI-4(10) Control Summary Information
Responsible Role:
Parameter SI-4(10)-1:
Parameter SI-4(10)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(10) What is the solution and how is it implemented?

SI-4(11) Analyze Communications Traffic Anomalies (H)

Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.

SI-4(11) Control Summary Information
Responsible Role:
Parameter SI-4(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(11) What is the solution and how is it implemented?

SI-4(12) Automated Organization-generated Alerts (H)

Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].

SI-4(12) Control Summary Information
Responsible Role:
Parameter SI-4(12)-1:
Parameter SI-4(12)-2:
Parameter SI-4(12)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(12) What is the solution and how is it implemented?

SI-4(14) Wireless Intrusion Detection (H)

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

SI-4(14) 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(14) What is the solution and how is it implemented?

SI-4(16) Correlate Monitoring Information (M)(H)

Correlate information from monitoring tools and mechanisms employed throughout the system.

SI-4(16) 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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(16) What is the solution and how is it implemented?

SI-4(18) Analyze Traffic and Covert Exfiltration (M)(H)

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].

SI-4(18) Control Summary Information
Responsible Role:
Parameter SI-4(18):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(18) What is the solution and how is it implemented?

SI-4(19) Risk for Individuals (H)

Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.

SI-4(19) Control Summary Information
Responsible Role:
Parameter SI-4(19)-1:

Parameter SI-4(19)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(19) What is the solution and how is it implemented?

SI-4(20) Privileged Users (H)

Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].

SI-4(20) Control Summary Information
Responsible Role:
Parameter SI-4(20):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(20) What is the solution and how is it implemented?

SI-4(22) Unauthorized Network Services (H)

(a) Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and

(b) [Selection (one-or-more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected.

SI-4(22) Control Summary Information
Responsible Role:
Parameter SI-4(22)(a):
Parameter SI-4(22)(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(22) What is the solution and how is it implemented?
Part a:
Part b:

SI-4(23) Host-based Devices (M)(H)

Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].

SI-4(23) Control Summary Information
Responsible Role:
Parameter SI-4(23)-1:
Parameter SI-4(23)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-4(23) What is the solution and how is it implemented?

SI-5 Security Alerts, Advisories, and Directives (L)(M)(H)

a. Receive system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT and Cybersecurity and Infrastructure Security Agency (CISA) Directives] on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: [Selection (one-or-more): [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

SI-5 Additional FedRAMP Requirements and Guidance:

Requirement: Service Providers must address the CISA Emergency and Binding Operational Directives applicable to their cloud service offering per FedRAMP guidance. This includes listing the applicable directives and stating compliance status.

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 FedRAMP 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-5(1) Automated Alerts and Advisories (H)

Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].

SI-5(1) Control Summary Information
Responsible Role:
Parameter SI-5(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-5(1) What is the solution and how is it implemented?

SI-6 Security and Privacy Function Verification (M)(H)

a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];

b. Perform the verification of the functions specified in SI-6a [FedRAMP Assignment: system transitional states to include upon system startup and/or restart; upon command by user with appropriate privilege]; [FedRAMP Assignment: at least monthly];

c. Alert [FedRAMP Assignment: to include system administrators and security personnel] to failed security and privacy verification tests; and

d. [Selection (one-or-more): Shut the system down; Restart the system; alternative actions(s)] when anomalies are discovered.

SI-6 Control Summary Information
Responsible Role:
Parameter SI-6(a):

Parameter SI-6(b):
Parameter SI-6(c):
Parameter SI-6(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-6 What is the solution and how is it implemented?
Part a:

Part b:
Part c:
Part d:

SI-7 Software, Firmware, and Information Integrity (M)(H)

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

SI-7 Control Summary Information
Responsible Role:
Parameter SI-7(a):
Parameter SI-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-7 What is the solution and how is it implemented?
Part a:
Part b:

SI-7(1) Integrity Checks (M)(H)

Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one-or-more): at startup; at [FedRAMP Assignment: selection to include security relevant events]; [FedRAMP Assignment: at least monthly]].

SI-7(1) Control Summary Information
Responsible Role:
Parameter SI-7(1)-1:
Parameter SI-7(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-7(1) What is the solution and how is it implemented?

SI-7(2) Automated Notifications of Integrity Violations (H)

Employ automated tools that provide notification to [FedRAMP Assignment: to include the ISSO and/or similar role within the organization] upon discovering discrepancies during integrity verification.

SI-7(2) Control Summary Information
Responsible Role:
Parameter SI-7(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-7(2) What is the solution and how is it implemented?

SI-7(5) Automated Response to Integrity Violations (H)

Automatically [Selection (one-or-more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.

SI-7(5) Control Summary Information
Responsible Role:
Parameter SI-7(5):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-7(5) What is the solution and how is it implemented?

SI-7(7) Integration of Detection and Response (M)(H)

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].

SI-7(7) Control Summary Information
Responsible Role:
Parameter SI-7(7):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-7(7) What is the solution and how is it implemented?

SI-7(15) Code Authentication (H)

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [FedRAMP Assignment: to include all software and firmware inside the boundary].

SI-7(15) Control Summary Information
Responsible Role:
Parameter SI-7(15):
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-7(15) What is the solution and how is it implemented?

SI-8 Spam Protection (M)(H)

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SI-8 Additional FedRAMP Requirements and Guidance:

Guidance: When CSO sends email on behalf of the government as part of the business offering, Control Description should include implementation of Domain-based Message Authentication, Reporting & Conformance (DMARC) on the sending domain for outgoing messages as described in DHS Binding Operational Directive (BOD) 18-01. https://cyber.dhs.gov/bod/18-01/.

Guidance: CSPs should confirm DMARC configuration (where appropriate) to ensure that policy=reject and the rua parameter includes reports@dmarc.cyber.dhs.gov. DMARC compliance should be documented in the SI-08 control implementation solution description, and list the FROM: domain(s) that will be seen by email recipients.

SI-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-8 What is the solution and how is it implemented?
Part a:
Part b:

SI-8(2) Automatic Updates (M)(H)

Automatically update spam protection mechanisms [Assignment: organization-defined frequency].

SI-8(2) Control Summary Information
Responsible Role:
Parameter SI-8(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

SI-10 Information Input Validation (M)(H)

Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].

SI-10 Additional FedRAMP Requirements and Guidance:

Requirement: Validate all information inputs and document any exceptions

SI-10 Control Summary Information
Responsible Role:
Parameter SI-10:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-10 What is the solution and how is it implemented?

SI-11 Error Handling (M)(H)

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to [FedRAMP Assignment: to include the ISSO and/or similar role within the organization].

SI-11 Control Summary Information
Responsible Role:
Parameter SI-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-11 What is the solution and how is it implemented?
Part a:
Part b:

SI-12 Information Management and Retention (L)(M)(H)

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines 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 FedRAMP 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 (M)(H)

Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].

SI-16 Control Summary Information

Responsible Role:
Parameter SI-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SI-16 What is the solution and how is it implemented?

Supply Chain Risk Management

SR-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [FedRAMP Assignment: to include chief privacy and ISSO and/or similar role or designees]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] supply chain risk management policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

   1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SR-1 Control Summary Information
Responsible Role:
Parameter SR-1(a):

Parameter SR-1(a)(1):
Parameter SR-1(b):
Parameter SR-1(c)(1)-1:
Parameter SR-1(c)(1)-2:
Parameter SR-1(c)(2)-1:
Parameter SR-1(c)(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)

SR-1 What is the solution and how is it implemented?
Part a:
Part b:

Part c:

SR-2 Supply Chain Risk Management Plan (L)(M)(H)

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services [Assignment: organization-defined systems, system components, or system services]

b. Review and update the supply chain risk management plan [FedRAMP Assignment: at least annually] or as required to address threat, organizational, or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2 Control Summary Information
Responsible Role:
Parameter SR-2(a):
Parameter SR-2(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-2 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SR-2(1) Establish SCRM Team (L)(M)(H)

Establish a supply chain risk management team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].

SR-2(1) Control Summary Information
Responsible Role:
Parameter SR-2(1)-1:

Parameter SR-2(1)-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

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

SR-3 Supply Chain Controls and Processes (L)(M)(H)

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and

c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan [Assignment: organization-defined document]].

SR-3 Additional FedRAMP Requirements and Guidance:

Requirement: CSO must document and maintain the supply chain custody, including replacement devices, to ensure the integrity of the devices before being introduced to the boundary.

SR-3 Control Summary Information
Responsible Role:
Parameter SR-3(a)-1:
Parameter SR-3(a)-2:
Parameter SR-3(b):
Parameter SR-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-3 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SR-5 Acquisition Strategies, Tools, and Methods (L)(M)(H)

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].

SR-5 Control Summary Information
Responsible Role:
Parameter SR-5:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-5 What is the solution and how is it implemented?

SR-6 Supplier Assessments and Reviews (M)(H)

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [FedRAMP Assignment: at least annually].

SR-6 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure that their supply chain vendors build and test their systems in alignment with NIST SP 800-171 or a commensurate security and compliance framework. CSOs must ensure that vendors are compliant with physical facility access and logical access controls to supplied products.

SR-6 Control Summary Information
Responsible Role:
Parameter SR-6:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-6 What is the solution and how is it implemented?

SR-8 Notification Agreements (L)(M)(H)

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [FedRAMP Assignment: notification of supply chain compromises and results of assessment or audits].

SR-8 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure and document how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities.

SR-8 Control Summary Information
Responsible Role:
Parameter SR-8:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-8 What is the solution and how is it implemented?

SR-9 Tamper Resistance and Detection (H)

Implement a tamper protection program for the system, system component, or system service.

SR-9 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure vendors provide authenticity of software and patches supplied to the service provider including documenting the safeguards in place.

SR-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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-9 What is the solution and how is it implemented?

SR-9(1) Multiple Stages of System Development Life Cycle (H)

Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

SR-9(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-9(1) What is the solution and how is it implemented?

SR-10 Inspection of Systems or Components (L)(M)(H)

Inspect the following systems or system components [Selection (one-or-more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].

SR-10 Control Summary Information
Responsible Role:
Parameter SR-10-1:
Parameter SR-10-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-10 What is the solution and how is it implemented?

SR-11 Component Authenticity (L)(M)(H)

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to [Selection (one-or-more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

SR-11 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure that their supply chain vendors provide authenticity of software and patches and the vendor must have a plan to protect the development pipeline.

SR-11 Control Summary Information
Responsible Role:
Parameter SR-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-11 What is the solution and how is it implemented?
Part a:
Part b:

SR-11(1) Anti-counterfeit Training (L)(M)(H)

Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).

SR-11(1) Control Summary Information
Responsible Role:
Parameter SR-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-11(1) What is the solution and how is it implemented?

SR-11(2) Configuration Control for Component Service and Repair (L)(M)(H)

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [FedRAMP Assignment: all].

SR-11(2) Control Summary Information
Responsible Role:
Parameter SR-11(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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-11(2) What is the solution and how is it implemented?

SR-12 Component Disposal (L)(M)(H)

Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].

SR-12 Control Summary Information
Responsible Role:
Parameter SR-12-1:
Parameter SR-12-2:
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 FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-12 What is the solution and how is it implemented?