**<EXTERNAL ENTITY NAME>**

Contract #: <TEXAS HHS CONTRACT NUMBER>

**<SYSTEM NAME>**

**<ASSESSMENT DATE>**

**Security Assessment Report**

<**Instructions**: Fill in all sections that have a bracket <> surrounding the text. All sections with a <> should be completed and the <> portions deleted prior to the Security Assessment Report being submitted to Texas HHS.>

# EXECUTIVE SUMMARY

A security assessment for <System Name>, herein referred to as the information system, was completed on <Assessment Date>. The purpose of this report is to provide a holistic summary of the risks that affect the confidentiality, integrity and availability of the information system and Texas HHS data that the information system creates, receives, processes, maintains, stores, or transmits.

## Security Assessment Report

The intent of the Security Assessment Report is to identify the current level of risk the information system poses to Texas HHS data. This report details the information system’s compliance with applicable Texas HHS security controls required per the security baseline as defined within the contract and detailed in the Texas HHS publication, Information Security Controls (IS-Controls).

<Delete the below if not applicable>

This security assessment is an update to the previous security assessment conducted on <Assessment Date>.

## Information System Security Baseline

The information system security baseline, as defined in the contract, is:

**Baseline:** <List only one>: Low, Low Plus, Moderate, High>

**Overlay:** <List zero or more: MARS-E, CJIS, IRS, SSA, FERPA, VA Mod, Select Agent, NCHHSTP, HIPAA, SPI, Web & Mobile>

<See the contract for the applicable baselines and overlays. If these are unknown contact the Texas HHS contract manager. Only Texas HHS can establish the applicable baselines.>

## Information System Description

<Provide a high level overview of the information system being assessed. Describe the business purpose, the types of Texas HHS data it receives, and what it does with the Texas HHS data>

## Security Assessor

<Fill in the contact information below>

This assessment was conducted by:

**Assessor Company:**

**Assessor Name:**

**Assessor Phone Number:**

**Assessor Email:**

**Assessor Address:**

<The following paragraph may be deleted if the system has a low or low plus baseline>

The security assessor meets the impartiality requirement stipulated in IS-Controls CA-02(01), *Independent Assessors*, and has no operational responsibility for the system being assessed[[1]](#footnote-2).

## Security Assessment Methodology

The overall framework used for this security assessment is found in the Texas HHS IS-Controls. <List any other assessment methodologies used to conduct the assessment>

## Summary of Security Assessment Results

The following was identified during the security assessment:

Number of Security Controls Required per Baseline/Overlays: <NUMBER>

Number of Security Controls Assessed: <NUMBER>

Number of Security Controls Not in Place: <NUMBER>

Number of Security Controls In Place: <NUMBER>

Number of Not-In-Place Controls in Previous Assessment: <NUMBER OR N/A>

Number of Newly Identified Not-in-Place Security Controls: <NUMBER>

# RESULTS

The security assessment identified <Input Number of Controls Not in Place> security controls out of <List Total Number of Controls the System Must Comply With> that were non-compliant with IS-Controls requirements.

## List of Non-Compliant Controls

The following security controls were identified as non-compliant. Each non-compliant security control identifies the assessment methodology used to assess the non-compliance and whether the security control failed the previous assessment.

This assessment methodologies are:

**E:** Examine

**I:** Interview

**T:** Test

See IS-Controls section 2.4.2 and NIST 800-53AR4 for further information on security assessments.

<Copy and paste the below table for each security control identified as non-compliant. The Control ID is the IS-Controls ID (e.g., AC-01) and the corresponding control name. For each control assessed enter an X in the table below to indicate the assessment methodology performed. If any of the security controls failed the previous assessment, mark Previously Failed Control as “Yes”, otherwise select “No”>

| Control | Control Name | E | I | T | Previously Failed Control |
| --- | --- | --- | --- | --- | --- |
| <Control ID> | <Control Name> |  |  |  | Choose an item. |
| **Finding:**<Explain why the security control is non-compliant> |

## Non-Compliance Update

The following security controls were identified as non-compliant within the security assessment conducted on <date of last assessment>. The following list details their current status.

<List only the controls that were previously non-compliant and their current status as either changed to “In Place” or left as “Not in Place”. If this is the first assessment, state that and delete the table below.>

| Control | Control Name | PreviousAssessment | CurrentAssessment |
| --- | --- | --- | --- |
| <Control ID> | <Control Name> | Not In Place | Choose an item. |
|  |  |  |  |

# Appendix A: Comprehensive List of Security Controls Assessed

<Delete all controls that do not apply to the information system based on the security baselines and overlays as identified in the contract. See IS-Controls and the applicable security baselines for the list of required security controls. For each control assessed enter an X for the type of assessment methodology used under Examine (E), Interview (I), and/or Test (T).

Additionally, for any control assessed indicate the implementation status of the control as either:

* In Place
* Not in Place

| Control | Control Name | E | I | T | Status |
| --- | --- | --- | --- | --- | --- |
| AC-01 | Access Control Policy And Procedures |  |  |  | Choose an item. |
| AC-02 | Account Management |  |  |  | Choose an item. |
| AC-02(01) | Automated System Account Management |  |  |  | Choose an item. |
| AC-02(02) | Removal Of Temporary / Emergency Accounts |  |  |  | Choose an item. |
| AC-02(03) | Disable Inactive Accounts |  |  |  | Choose an item. |
| AC-02(04) | Automated Audit Actions |  |  |  | Choose an item. |
| AC-02(07) | Role-Based Schemes |  |  |  | Choose an item. |
| AC-03 | Access Enforcement |  |  |  | Choose an item. |
| AC-03(03) | Mandatory Access Control |  |  |  | Choose an item. |
| AC-03(04) | Discretionary Access Control |  |  |  | Choose an item. |
| AC-03(09) | Controlled Release |  |  |  | Choose an item. |
| AC-04 | Information Flow Enforcement |  |  |  | Choose an item. |
| AC-05 | Separation Of Duties |  |  |  | Choose an item. |
| AC-06 | Least Privilege |  |  |  | Choose an item. |
| AC-06(01) | Authorize Access To Security Functions |  |  |  | Choose an item. |
| AC-06(02) | Non-Privileged Access For Nonsecurity Functions |  |  |  | Choose an item. |
| AC-06(05) | Privileged Accounts |  |  |  | Choose an item. |
| AC-06(09) | Auditing Use Of Privileged Functions |  |  |  | Choose an item. |
| AC-06(10) | Prohibit Non-Privileged Users From Executing Privileged Functions |  |  |  | Choose an item. |
| AC-07 | Unsuccessful Logon Attempts |  |  |  | Choose an item. |
| AC-07(02) | Purge / Wipe Mobile Device |  |  |  | Choose an item. |
| AC-08 | System Use Notification |  |  |  | Choose an item. |
| AC-09 | Previous Logon (Access) Notification |  |  |  | Choose an item. |
| AC-10 | Concurrent Session Control |  |  |  | Choose an item. |
| AC-11 | Session Lock |  |  |  | Choose an item. |
| AC-11(01) | Pattern-Hiding Displays |  |  |  | Choose an item. |
| AC-12 | Session Termination |  |  |  | Choose an item. |
| AC-12(01) | User-Initiated Logouts / Message Displays |  |  |  | Choose an item. |
| AC-14 | Permitted Actions Without Identification Or Authentication |  |  |  | Choose an item. |
| AC-16 | Security Attributes |  |  |  | Choose an item. |
| AC-17 | Remote Access |  |  |  | Choose an item. |
| AC-17(01) | Automated Monitoring / Control |  |  |  | Choose an item. |
| AC-17(02) | Protection Of Confidentiality / Integrity Using Encryption |  |  |  | Choose an item. |
| AC-17(03) | Managed Access Control Points |  |  |  | Choose an item. |
| AC-17(04) | Privileged Commands / Access |  |  |  | Choose an item. |
| AC-17(06) | Protection Of Information |  |  |  | Choose an item. |
| AC-18 | Wireless Access |  |  |  | Choose an item. |
| AC-18(01) | Authentication And Encryption |  |  |  | Choose an item. |
| AC-18(05) | Antennas / Transmission Power Levels |  |  |  | Choose an item. |
| AC-19 | Access Control For Mobile Devices |  |  |  | Choose an item. |
| AC-19(05) | Full Device / Container-Based Encryption |  |  |  | Choose an item. |
| AC-20 | Use Of External Information Systems |  |  |  | Choose an item. |
| AC-20(01) | Limits On Authorized Use |  |  |  | Choose an item. |
| AC-20(02) | Portable Storage Devices |  |  |  | Choose an item. |
| AC-20(03) | Non-Organizationally Owned Systems / Components / Devices |  |  |  | Choose an item. |
| AC-21 | Information Sharing |  |  |  | Choose an item. |
| AC-22 | Publicly Accessible Content |  |  |  | Choose an item. |
| AC-23 | Data Mining Protection |  |  |  | Choose an item. |
| AT-01 | Security Awareness And Training Policy And Procedures |  |  |  | Choose an item. |
| AT-02 | Security Awareness Training |  |  |  | Choose an item. |
| AT-02(02) | Insider Threat |  |  |  | Choose an item. |
| AT-03 | Role-Based Security Training |  |  |  | Choose an item. |
| AT-04 | Security Training Records |  |  |  | Choose an item. |
| AU-01 | Audit And Accountability Policy And Procedures |  |  |  | Choose an item. |
| AU-02 | Audit Events |  |  |  | Choose an item. |
| AU-02(03) | Reviews And Updates |  |  |  | Choose an item. |
| AU-03 | Content Of Audit Records |  |  |  | Choose an item. |
| AU-03(01) | Additional Audit Information |  |  |  | Choose an item. |
| AU-04 | Audit Storage Capacity |  |  |  | Choose an item. |
| AU-05 | Response To Audit Processing Failures |  |  |  | Choose an item. |
| AU-05(01) | Audit Storage Capacity |  |  |  | Choose an item. |
| AU-05(02) | Real-Time Alerts |  |  |  | Choose an item. |
| AU-06 | Audit Review, Analysis, And Reporting |  |  |  | Choose an item. |
| AU-06(01) | Process Integration |  |  |  | Choose an item. |
| AU-06(03) | Correlate Audit Repositories |  |  |  | Choose an item. |
| AU-07 | Audit Reduction And Report Generation |  |  |  | Choose an item. |
| AU-07(01) | Automatic Processing |  |  |  | Choose an item. |
| AU-08 | Time Stamps |  |  |  | Choose an item. |
| AU-08(01) | Synchronization With Authoritative Time Source |  |  |  | Choose an item. |
| AU-09 | Protection Of Audit Information |  |  |  | Choose an item. |
| AU-09(02) | Audit Backup On Separate Physical Systems / Components |  |  |  | Choose an item. |
| AU-09(04) | Access By Subset Of Privileged Users |  |  |  | Choose an item. |
| AU-10 | Non-Repudiation |  |  |  | Choose an item. |
| AU-11 | Audit Record Retention |  |  |  | Choose an item. |
| AU-12 | Audit Generation |  |  |  | Choose an item. |
| AU-12(01) | System-Wide / Time-Correlated Audit Trail |  |  |  | Choose an item. |
| AU-13 | Monitoring For Information Disclosure |  |  |  | Choose an item. |
| AU-16 | Cross-Organizational Auditing |  |  |  | Choose an item. |
| CA-01 | Security Assessment And Authorization Policy And Procedures |  |  |  | Choose an item. |
| CA-02 | Security Assessments |  |  |  | Choose an item. |
| CA-02(01) | Independent Assessors |  |  |  | Choose an item. |
| CA-03 | System Interconnections |  |  |  | Choose an item. |
| CA-03(01) | Unclassified National Security System Connections |  |  |  | Choose an item. |
| CA-03(02) | Classified National Security System Connections |  |  |  | Choose an item. |
| CA-03(05) | Restrictions On External System Connections |  |  |  | Choose an item. |
| CA-05 | Plan Of Action And Milestones |  |  |  | Choose an item. |
| CA-05(01) | Automation Support For Accuracy / Currency |  |  |  | Choose an item. |
| CA-06 | Security Authorization |  |  |  | Choose an item. |
| CA-07 | Continuous Monitoring |  |  |  | Choose an item. |
| CA-07(01) | Independent Assessment |  |  |  | Choose an item. |
| CA-08 | Penetration Testing |  |  |  | Choose an item. |
| CA-09 | Internal System Connections |  |  |  | Choose an item. |
| CM-01 | Configuration Management Policy And Procedures |  |  |  | Choose an item. |
| CM-02 | Baseline Configuration |  |  |  | Choose an item. |
| CM-02(01) | Reviews And Updates |  |  |  | Choose an item. |
| CM-02(03) | Retention Of Previous Configurations |  |  |  | Choose an item. |
| CM-02(07) | Configure Systems, Components, Or Devices For High-Risk Areas |  |  |  | Choose an item. |
| CM-03 | Configuration Change Control |  |  |  | Choose an item. |
| CM-03(01) | Automated Document / Notification / Prohibition Of Changes |  |  |  | Choose an item. |
| CM-03(02) | Test / Validate / Document Changes |  |  |  | Choose an item. |
| CM-03(04) | Security Representative |  |  |  | Choose an item. |
| CM-04 | Security Impact Analysis |  |  |  | Choose an item. |
| CM-04(01) | Separate Test Environments |  |  |  | Choose an item. |
| CM-04(02) | Verification Of Security Functions |  |  |  | Choose an item. |
| CM-05 | Access Restrictions For Change |  |  |  | Choose an item. |
| CM-05(01) | Automated Access Enforcement / Auditing |  |  |  | Choose an item. |
| CM-05(02) | Review System Changes |  |  |  | Choose an item. |
| CM-05(05) | Limit Production / Operational Privileges |  |  |  | Choose an item. |
| CM-05(06) | Limit Library Privileges |  |  |  | Choose an item. |
| CM-06 | Configuration Settings |  |  |  | Choose an item. |
| CM-06(01) | Automated Central Management / Application / Verification |  |  |  | Choose an item. |
| CM-07 | Least Functionality |  |  |  | Choose an item. |
| CM-07(01) | Periodic Review |  |  |  | Choose an item. |
| CM-07(02) | Prevent Program Execution |  |  |  | Choose an item. |
| CM-07(03) | Registration Compliance |  |  |  | Choose an item. |
| CM-07(04) | Unauthorized Software / Blacklisting |  |  |  | Choose an item. |
| CM-07(05) | Authorized Software / Whitelisting |  |  |  | Choose an item. |
| CM-08 | Information System Component Inventory |  |  |  | Choose an item. |
| CM-08(01) | Updates During Installations / Removals |  |  |  | Choose an item. |
| CM-08(03) | Automated Unauthorized Component Detection |  |  |  | Choose an item. |
| CM-08(05) | No Duplicate Accounting Of Components |  |  |  | Choose an item. |
| CM-09 | Configuration Management Plan |  |  |  | Choose an item. |
| CM-10 | Software Usage Restrictions |  |  |  | Choose an item. |
| CM-10(01) | Open Source Software |  |  |  | Choose an item. |
| CM-11 | User-Installed Software |  |  |  | Choose an item. |
| CP-01 | Contingency Planning Policy And Procedures |  |  |  | Choose an item. |
| CP-02 | Contingency Plan |  |  |  | Choose an item. |
| CP-02(01) | Coordinate With Related Plans |  |  |  | Choose an item. |
| CP-02(02) | Capacity Planning |  |  |  | Choose an item. |
| CP-02(03) | Resume Essential Missions / Business Functions |  |  |  | Choose an item. |
| CP-02(05) | Continue Essential Missions / Business Functions |  |  |  | Choose an item. |
| CP-02(08) | Identify Critical Assets |  |  |  | Choose an item. |
| CP-03 | Contingency Training |  |  |  | Choose an item. |
| CP-04 | Contingency Plan Testing |  |  |  | Choose an item. |
| CP-04(01) | Coordinate With Related Plans |  |  |  | Choose an item. |
| CP-06 | Alternate Storage Site |  |  |  | Choose an item. |
| CP-06(01) | Separation From Primary Site |  |  |  | Choose an item. |
| CP-06(03) | Accessibility |  |  |  | Choose an item. |
| CP-07 | Alternate Processing Site |  |  |  | Choose an item. |
| CP-07(01) | Separation From Primary Site |  |  |  | Choose an item. |
| CP-07(02) | Accessibility |  |  |  | Choose an item. |
| CP-07(03) | Priority Of Service |  |  |  | Choose an item. |
| CP-08 | Telecommunications Services |  |  |  | Choose an item. |
| CP-08(01) | Priority Of Service Provisions |  |  |  | Choose an item. |
| CP-08(02) | Single Points Of Failure |  |  |  | Choose an item. |
| CP-09 | Information System Backup |  |  |  | Choose an item. |
| CP-09(01) | Testing For Reliability / Integrity |  |  |  | Choose an item. |
| CP-10 | Information System Recovery And Reconstitution |  |  |  | Choose an item. |
| CP-10(02) | Transaction Recovery |  |  |  | Choose an item. |
| CP-11 | Alternate Communications Protocols |  |  |  | Choose an item. |
| IA-01 | Identification And Authentication Policy And Procedures |  |  |  | Choose an item. |
| IA-02 | Identification And Authentication (Organizational Users) |  |  |  | Choose an item. |
| IA-02(01) | Network Access To Privileged Accounts |  |  |  | Choose an item. |
| IA-02(02) | Network Access To Non-Privileged Accounts |  |  |  | Choose an item. |
| IA-02(03) | Local Access To Privileged Accounts |  |  |  | Choose an item. |
| IA-02(04) | Local Access To Non-Privileged Accounts |  |  |  | Choose an item. |
| IA-02(05) | Group Authentication |  |  |  | Choose an item. |
| IA-02(08) | Network Access To Privileged Accounts - Replay Resistant |  |  |  | Choose an item. |
| IA-02(09) | Network Access To Non-Privileged Accounts - Replay Resistant |  |  |  | Choose an item. |
| IA-02(11) | Remote Access - Separate Device |  |  |  | Choose an item. |
| IA-02(12) | Acceptance Of Piv Credentials |  |  |  | Choose an item. |
| IA-02(13) | Out-Of-Band Authentication |  |  |  | Choose an item. |
| IA-03 | Device Identification And Authentication |  |  |  | Choose an item. |
| IA-03(01) | Cryptographic Bidirectional Authentication |  |  |  | Choose an item. |
| IA-03(04) | Device Attestation |  |  |  | Choose an item. |
| IA-04 | Identifier Management |  |  |  | Choose an item. |
| IA-04(02) | Supervisor Authorization |  |  |  | Choose an item. |
| IA-04(04) | Identify User Status |  |  |  | Choose an item. |
| IA-05 | Authenticator Management |  |  |  | Choose an item. |
| IA-05(01) | Password-Based Authentication |  |  |  | Choose an item. |
| IA-05(02) | Pki-Based Authentication |  |  |  | Choose an item. |
| IA-05(03) | In-Person Or Trusted Third-Party Registration |  |  |  | Choose an item. |
| IA-05(05) | Change Authenticators Prior To Delivery |  |  |  | Choose an item. |
| IA-05(06) | Protection Of Authenticators |  |  |  | Choose an item. |
| IA-05(07) | No Embedded Unencrypted Static Authenticators |  |  |  | Choose an item. |
| IA-05(08) | Multiple Information System Accounts |  |  |  | Choose an item. |
| IA-05(11) | Hardware Token-Based Authentication |  |  |  | Choose an item. |
| IA-06 | Authenticator Feedback |  |  |  | Choose an item. |
| IA-07 | Cryptographic Module Authentication |  |  |  | Choose an item. |
| IA-08 | Identification And Authentication (Non-Organizational Users) |  |  |  | Choose an item. |
| IA-08(01) | Acceptance Of Piv Credentials From Other Agencies |  |  |  | Choose an item. |
| IA-08(02) | Acceptance Of Third-Party Credentials |  |  |  | Choose an item. |
| IA-08(03) | Use Of Ficam-Approved Products |  |  |  | Choose an item. |
| IA-08(04) | Use Of Ficam-Issued Profiles |  |  |  | Choose an item. |
| IR-01 | Incident Response Policy And Procedures |  |  |  | Choose an item. |
| IR-02 | Incident Response Training |  |  |  | Choose an item. |
| IR-03 | Incident Response Testing |  |  |  | Choose an item. |
| IR-03(02) | Coordination With Related Plans |  |  |  | Choose an item. |
| IR-04 | Incident Handling |  |  |  | Choose an item. |
| IR-04(01) | Automated Incident Handling Processes |  |  |  | Choose an item. |
| IR-04(03) | Continuity Of Operations |  |  |  | Choose an item. |
| IR-04(04) | Information Correlation |  |  |  | Choose an item. |
| IR-05 | Incident Monitoring |  |  |  | Choose an item. |
| IR-06 | Incident Reporting |  |  |  | Choose an item. |
| IR-06(01) | Automated Reporting |  |  |  | Choose an item. |
| IR-06(02) | Vulnerabilities Related To Incidents |  |  |  | Choose an item. |
| IR-07 | Incident Response Assistance |  |  |  | Choose an item. |
| IR-07(01) | Automation Support For Availability Of Information / Support |  |  |  | Choose an item. |
| IR-07(02) | Coordination With External Providers |  |  |  | Choose an item. |
| IR-08 | Incident Response Plan |  |  |  | Choose an item. |
| IR-09 | Information Spillage Response |  |  |  | Choose an item. |
| MA-01 | System Maintenance Policy And Procedures |  |  |  | Choose an item. |
| MA-02 | Controlled Maintenance |  |  |  | Choose an item. |
| MA-03 | Maintenance Tools |  |  |  | Choose an item. |
| MA-03(01) | Inspect Tools |  |  |  | Choose an item. |
| MA-03(02) | Inspect Media |  |  |  | Choose an item. |
| MA-03(03) | Prevent Unauthorized Removal |  |  |  | Choose an item. |
| MA-04 | Nonlocal Maintenance |  |  |  | Choose an item. |
| MA-04(01) | Auditing And Review |  |  |  | Choose an item. |
| MA-04(02) | Document Nonlocal Maintenance |  |  |  | Choose an item. |
| MA-04(03) | Comparable Security / Sanitization |  |  |  | Choose an item. |
| MA-04(06) | Cryptographic Protection |  |  |  | Choose an item. |
| MA-04(07) | Remote Disconnect Verification |  |  |  | Choose an item. |
| MA-05 | Maintenance Personnel |  |  |  | Choose an item. |
| MA-05(04) | Foreign Nationals |  |  |  | Choose an item. |
| MA-06 | Timely Maintenance |  |  |  | Choose an item. |
| MP-01 | Media Protection Policy And Procedures |  |  |  | Choose an item. |
| MP-02 | Media Access |  |  |  | Choose an item. |
| MP-03 | Media Marking |  |  |  | Choose an item. |
| MP-04 | Media Storage |  |  |  | Choose an item. |
| MP-05 | Media Transport |  |  |  | Choose an item. |
| MP-05(04) | Cryptographic Protection |  |  |  | Choose an item. |
| MP-06 | Media Sanitization |  |  |  | Choose an item. |
| MP-06(01) | Review / Approve / Track / Document / Verify |  |  |  | Choose an item. |
| MP-06(02) | Equipment Testing |  |  |  | Choose an item. |
| MP-06(03) | Nondestructive Techniques |  |  |  | Choose an item. |
| MP-07 | Media Use |  |  |  | Choose an item. |
| MP-07(01) | Prohibit Use Without Owner |  |  |  | Choose an item. |
| MP-CMS-01 | Media Related Records |  |  |  | Choose an item. |
| PE-01 | Physical And Environmental Protection Policy And Procedures |  |  |  | Choose an item. |
| PE-02 | Physical Access Authorizations |  |  |  | Choose an item. |
| PE-02(01) | Access By Position / Role |  |  |  | Choose an item. |
| PE-02(03) | Restrict Unescorted Access |  |  |  | Choose an item. |
| PE-03 | Physical Access Control |  |  |  | Choose an item. |
| PE-03(02) | Facility / Information System Boundaries |  |  |  | Choose an item. |
| PE-03(03) | Continuous Guards / Alarms / Monitoring |  |  |  | Choose an item. |
| PE-04 | Access Control For Transmission Medium |  |  |  | Choose an item. |
| PE-05 | Access Control For Output Devices |  |  |  | Choose an item. |
| PE-06 | Monitoring Physical Access |  |  |  | Choose an item. |
| PE-06(01) | Intrusion Alarms / Surveillance Equipment |  |  |  | Choose an item. |
| PE-08 | Visitor Access Records |  |  |  | Choose an item. |
| PE-09 | Power Equipment And Cabling |  |  |  | Choose an item. |
| PE-10 | Emergency Shutoff |  |  |  | Choose an item. |
| PE-11 | Emergency Power |  |  |  | Choose an item. |
| PE-12 | Emergency Lighting |  |  |  | Choose an item. |
| PE-13 | Fire Protection |  |  |  | Choose an item. |
| PE-13(01) | Detection Devices / Systems |  |  |  | Choose an item. |
| PE-13(02) | Suppression Devices / Systems |  |  |  | Choose an item. |
| PE-13(03) | Automatic Fire Suppression |  |  |  | Choose an item. |
| PE-14 | Temperature And Humidity Controls |  |  |  | Choose an item. |
| PE-15 | Water Damage Protection |  |  |  | Choose an item. |
| PE-16 | Delivery And Removal |  |  |  | Choose an item. |
| PE-17 | Alternate Work Site |  |  |  | Choose an item. |
| PE-18 | Location Of Information System Components |  |  |  | Choose an item. |
| PE-18(01) | Facility Site |  |  |  | Choose an item. |
| PE-19 | Information Leakage |  |  |  | Choose an item. |
| PE-20 | Asset Monitoring And Tracking |  |  |  | Choose an item. |
| PL-01 | Security Planning Policy And Procedures |  |  |  | Choose an item. |
| PL-02 | System Security Plan |  |  |  | Choose an item. |
| PL-02(03) | Plan / Coordinate With Other Organizational Entities |  |  |  | Choose an item. |
| PL-04 | Rules Of Behavior |  |  |  | Choose an item. |
| PL-04(01) | Social Media And Networking Restrictions |  |  |  | Choose an item. |
| PL-07 | Security Concept Of Operations |  |  |  | Choose an item. |
| PL-08 | Information Security Architecture |  |  |  | Choose an item. |
| PL-09 | Central Management |  |  |  | Choose an item. |
| PS-01 | Personnel Security Policy And Procedures |  |  |  | Choose an item. |
| PS-02 | Position Risk Designation |  |  |  | Choose an item. |
| PS-03 | Personnel Screening |  |  |  | Choose an item. |
| PS-03(01) | Classified Information |  |  |  | Choose an item. |
| PS-03(02) | Formal Indoctrination |  |  |  | Choose an item. |
| PS-03(03) | Information With Special Protection Measures |  |  |  | Choose an item. |
| PS-04 | Personnel Termination |  |  |  | Choose an item. |
| PS-05 | Personnel Transfer |  |  |  | Choose an item. |
| PS-06 | Access Agreements |  |  |  | Choose an item. |
| PS-06(02) | Classified Information Requiring Special Protection |  |  |  | Choose an item. |
| PS-07 | Third-Party Personnel Security |  |  |  | Choose an item. |
| PS-08 | Personnel Sanctions |  |  |  | Choose an item. |
| RA-01 | Risk Assessment Policy And Procedures |  |  |  | Choose an item. |
| RA-02 | Security Categorization |  |  |  | Choose an item. |
| RA-03 | Risk Assessment |  |  |  | Choose an item. |
| RA-05 | Vulnerability Scanning |  |  |  | Choose an item. |
| RA-05(01) | Update Tool Capability |  |  |  | Choose an item. |
| RA-05(02) | Update By Frequency / Prior To New Scan / When Identified |  |  |  | Choose an item. |
| RA-05(03) | Breadth / Depth Of Coverage |  |  |  | Choose an item. |
| RA-05(05) | Privileged Access |  |  |  | Choose an item. |
| SA-01 | System And Services Acquisition Policy And Procedures |  |  |  | Choose an item. |
| SA-02 | Allocation Of Resources |  |  |  | Choose an item. |
| SA-03 | System Development Life Cycle |  |  |  | Choose an item. |
| SA-04 | Acquisition Process |  |  |  | Choose an item. |
| SA-04(01) | Functional Properties Of Security Controls |  |  |  | Choose an item. |
| SA-04(02) | Design / Implementation Information For Security Controls |  |  |  | Choose an item. |
| SA-04(09) | Functions / Ports / Protocols / Services In Use |  |  |  | Choose an item. |
| SA-04(10) | Use Of Approved Piv Products |  |  |  | Choose an item. |
| SA-05 | Information System Documentation |  |  |  | Choose an item. |
| SA-08 | Security Engineering Principles |  |  |  | Choose an item. |
| SA-09 | External Information System Services |  |  |  | Choose an item. |
| SA-09(01) | Risk Assessments / Organizational Approvals |  |  |  | Choose an item. |
| SA-09(02) | Identification Of Functions / Ports / Protocols / Services |  |  |  | Choose an item. |
| SA-09(05) | Processing, Storage, And Service Location |  |  |  | Choose an item. |
| SA-10 | Developer Configuration Management |  |  |  | Choose an item. |
| SA-11 | Developer Security Testing And Evaluation |  |  |  | Choose an item. |
| SA-11(01) | Static Code Analysis |  |  |  | Choose an item. |
| SA-11(02) | Threat And Vulnerability Analyses |  |  |  | Choose an item. |
| SA-11(05) | Penetration Testing |  |  |  | Choose an item. |
| SA-11(08) | Dynamic Code Analysis |  |  |  | Choose an item. |
| SA-12 | Supply Chain Protection |  |  |  | Choose an item. |
| SA-12(02) | Supplier Reviews |  |  |  | Choose an item. |
| SA-14 | Criticality Analysis |  |  |  | Choose an item. |
| SA-15 | Development Process, Standards, And Tools |  |  |  | Choose an item. |
| SA-17 | Developer Security Architecture And Design |  |  |  | Choose an item. |
| SA-22 | Unsupported System Components |  |  |  | Choose an item. |
| SC-01 | System And Communications Protection Policy And Procedures |  |  |  | Choose an item. |
| SC-02 | Application Partitioning |  |  |  | Choose an item. |
| SC-02(01) | Interfaces For Non-Privileged Users |  |  |  | Choose an item. |
| SC-03 | Security Function Isolation |  |  |  | Choose an item. |
| SC-04 | Information In Shared Resources |  |  |  | Choose an item. |
| SC-05 | Denial Of Service Protection |  |  |  | Choose an item. |
| SC-05(01) | Restrict Internal Users |  |  |  | Choose an item. |
| SC-05(02) | Excess Capacity / Bandwidth / Redundancy |  |  |  | Choose an item. |
| SC-05(03) | Detection / Monitoring |  |  |  | Choose an item. |
| SC-06 | Resource Availability |  |  |  | Choose an item. |
| SC-07 | Boundary Protection |  |  |  | Choose an item. |
| SC-07(03) | Access Points |  |  |  | Choose an item. |
| SC-07(04) | External Telecommunications Services |  |  |  | Choose an item. |
| SC-07(05) | Deny By Default / Allow By Exception |  |  |  | Choose an item. |
| SC-07(07) | Prevent Split Tunneling For Remote Devices |  |  |  | Choose an item. |
| SC-07(08) | Route Traffic To Authenticated Proxy Servers |  |  |  | Choose an item. |
| SC-07(11) | Restrict Incoming Communications Traffic |  |  |  | Choose an item. |
| SC-07(12) | Host-Based Protection |  |  |  | Choose an item. |
| SC-07(13) | Isolation Of Security Tools / Mechanisms / Support Components |  |  |  | Choose an item. |
| SC-07(14) | Protects Against Unauthorized Physical Connections |  |  |  | Choose an item. |
| SC-07(18) | Fail Secure |  |  |  | Choose an item. |
| SC-07(19) | Blocks Communication From Non-Organizationally Configured Hosts |  |  |  | Choose an item. |
| SC-08 | Transmission Confidentiality And Integrity |  |  |  | Choose an item. |
| SC-08(01) | Cryptographic Or Alternate Physical Protection |  |  |  | Choose an item. |
| SC-08(02) | Pre / Post Transmission Handling |  |  |  | Choose an item. |
| SC-10 | Network Disconnect |  |  |  | Choose an item. |
| SC-11 | Trusted Path |  |  |  | Choose an item. |
| SC-12 | Cryptographic Key Establishment And Management |  |  |  | Choose an item. |
| SC-12(01) | Availability |  |  |  | Choose an item. |
| SC-12(02) | Symmetric Keys |  |  |  | Choose an item. |
| SC-12(03) | Asymmetric Keys |  |  |  | Choose an item. |
| SC-13 | Cryptographic Protection |  |  |  | Choose an item. |
| SC-15 | Collaborative Computing Devices |  |  |  | Choose an item. |
| SC-15(01) | Physical Disconnect |  |  |  | Choose an item. |
| SC-16 | Transmission Of Security Attributes |  |  |  | Choose an item. |
| SC-16(01) | Integrity Validation |  |  |  | Choose an item. |
| SC-17 | Public Key Infrastructure Certificates |  |  |  | Choose an item. |
| SC-18 | Mobile Code |  |  |  | Choose an item. |
| SC-18(01) | Identify Unacceptable Code / Take Corrective Actions |  |  |  | Choose an item. |
| SC-18(02) | Acquisition / Development / Use |  |  |  | Choose an item. |
| SC-18(03) | Prevent Downloading / Execution |  |  |  | Choose an item. |
| SC-18(04) | Prevent Automatic Execution |  |  |  | Choose an item. |
| SC-19 | Voice Over Internet Protocol |  |  |  | Choose an item. |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) |  |  |  | Choose an item. |
| SC-21 | Secure Name / Address Resolution Service (Recursive Or Caching Resolver) |  |  |  | Choose an item. |
| SC-22 | Architecture And Provisioning For Name / Address Resolution Service |  |  |  | Choose an item. |
| SC-23 | Session Authenticity |  |  |  | Choose an item. |
| SC-23(01) | Invalidate Session Identifiers At Logout |  |  |  | Choose an item. |
| SC-23(03) | Unique Session Identifiers With Randomization |  |  |  | Choose an item. |
| SC-24 | Fail In Known State |  |  |  | Choose an item. |
| SC-28 | Protection Of Information At Rest |  |  |  | Choose an item. |
| SC-28(01) | Cryptographic Protection |  |  |  | Choose an item. |
| SC-31 | Covert Channel Analysis |  |  |  | Choose an item. |
| SC-32 | Information System Partitioning |  |  |  | Choose an item. |
| SC-36 | Distributed Processing And Storage |  |  |  | Choose an item. |
| SC-37 | Out-Of-Band Channels |  |  |  | Choose an item. |
| SC-37(01) | Ensure Delivery / Transmission |  |  |  | Choose an item. |
| SC-38 | Operations Security |  |  |  | Choose an item. |
| SC-39 | Process Isolation |  |  |  | Choose an item. |
| SC-40 | Wireless Link Protection |  |  |  | Choose an item. |
| SC-43 | Usage Restrictions |  |  |  | Choose an item. |
| SC-44 | Detonation Chambers |  |  |  | Choose an item. |
| SC-ACA-01 | Electronic Mail |  |  |  | Choose an item. |
| SC-ACA-02 | Fax Usage |  |  |  | Choose an item. |
| SI-01 | System And Information Integrity Policy And Procedures |  |  |  | Choose an item. |
| SI-02 | Flaw Remediation |  |  |  | Choose an item. |
| SI-02(01) | Central Management |  |  |  | Choose an item. |
| SI-02(02) | Automated Flaw Remediation Status |  |  |  | Choose an item. |
| SI-02(03) | Time To Remediate Flaws / Benchmarks For Corrective Actions |  |  |  | Choose an item. |
| SI-03 | Malicious Code Protection |  |  |  | Choose an item. |
| SI-03(01) | Central Management |  |  |  | Choose an item. |
| SI-03(02) | Automatic Updates |  |  |  | Choose an item. |
| SI-04 | Information System Monitoring |  |  |  | Choose an item. |
| SI-04(01) | System-Wide Intrusion Detection System |  |  |  | Choose an item. |
| SI-04(02) | Automated Tools For Real-Time Analysis |  |  |  | Choose an item. |
| SI-04(04) | Inbound And Outbound Communications Traffic |  |  |  | Choose an item. |
| SI-04(05) | System-Generated Alerts |  |  |  | Choose an item. |
| SI-04(07) | Automated Response To Suspicious Events |  |  |  | Choose an item. |
| SI-04(09) | Testing Of Monitoring Tools |  |  |  | Choose an item. |
| SI-04(11) | Analyze Communications Traffic Anomalies |  |  |  | Choose an item. |
| SI-04(12) | Automated Alerts |  |  |  | Choose an item. |
| SI-04(14) | Wireless Intrusion Detection |  |  |  | Choose an item. |
| SI-04(15) | Wireless To Wireline Communications |  |  |  | Choose an item. |
| SI-04(23) | Host-Based Devices |  |  |  | Choose an item. |
| SI-05 | Security Alerts, Advisories, And Directives |  |  |  | Choose an item. |
| SI-05(01) | Automated Alerts And Advisories |  |  |  | Choose an item. |
| SI-06 | Security Function Verification |  |  |  | Choose an item. |
| SI-07 | Software, Firmware, And Information Integrity |  |  |  | Choose an item. |
| SI-07(01) | Integrity Checks |  |  |  | Choose an item. |
| SI-07(07) | Integration Of Detection And Response |  |  |  | Choose an item. |
| SI-08 | Spam Protection |  |  |  | Choose an item. |
| SI-08(01) | Central Management |  |  |  | Choose an item. |
| SI-08(02) | Automatic Updates |  |  |  | Choose an item. |
| SI-10 | Information Input Validation |  |  |  | Choose an item. |
| SI-11 | Error Handling |  |  |  | Choose an item. |
| SI-12 | Information Handling And Retention |  |  |  | Choose an item. |
| SI-16 | Memory Protection |  |  |  | Choose an item. |
| PM-01 | Information Security Program Plan |  |  |  | Choose an item. |
| PM-02 | Senior Information Security Officer |  |  |  | Choose an item. |
| PM-03 | Information Security Resources |  |  |  | Choose an item. |
| PM-04 | Plan Of Action And Milestones Process |  |  |  | Choose an item. |
| PM-05 | Information System Inventory |  |  |  | Choose an item. |
| PM-06 | Information Security Measures Of Performance |  |  |  | Choose an item. |
| PM-07 | Enterprise Architecture |  |  |  | Choose an item. |
| PM-08 | Critical Infrastructure Plan |  |  |  | Choose an item. |
| PM-09 | Risk Management Strategy |  |  |  | Choose an item. |
| PM-10 | Security Authorization Process |  |  |  | Choose an item. |
| PM-11 | Mission/Business Process Definition |  |  |  | Choose an item. |
| PM-12 | Insider Threat Program |  |  |  | Choose an item. |
| PM-13 | Information Security Workforce |  |  |  | Choose an item. |
| PM-14 | Testing, Training, And Monitoring |  |  |  | Choose an item. |
| PM-15 | Contacts With Security Groups And Associations |  |  |  | Choose an item. |
| PM-16 | Threat Awareness Program |  |  |  | Choose an item. |
| AP-01 | Authority To Collect |  |  |  | Choose an item. |
| AP-02 | Purpose Specification |  |  |  | Choose an item. |
| AR-01 | Governance And Privacy Program |  |  |  | Choose an item. |
| AR-02 | Privacy Impact And Risk Assessment |  |  |  | Choose an item. |
| AR-03 | Privacy Requirements For Contractors And Service Providers |  |  |  | Choose an item. |
| AR-04 | Privacy Monitoring And Auditing |  |  |  | Choose an item. |
| AR-05 | Privacy Awareness And Training |  |  |  | Choose an item. |
| AR-06 | Privacy Reporting |  |  |  | Choose an item. |
| AR-07 | Privacy-Enhanced System Design And Development |  |  |  | Choose an item. |
| AR-08 | Accounting Of Disclosures |  |  |  | Choose an item. |
| DI-01 | Data Quality |  |  |  | Choose an item. |
| DI-01(01) | Validate Pii |  |  |  | Choose an item. |
| DI-02 | Data Integrity And Data Integrity Board |  |  |  | Choose an item. |
| DI-02(01) | Publish Agreements On Websites |  |  |  | Choose an item. |
| DM-01 | Minimization Of Personally Identifiable Information |  |  |  | Choose an item. |
| DM-01(01) | Minimization Of Personally Identifiable Information |  |  |  | Choose an item. |
| DM-02 | Data Retention And Disposal |  |  |  | Choose an item. |
| DM-02(01) | System Configuration |  |  |  | Choose an item. |
| DM-03 | Minimization Of Pii Used In Testing, Training, And Research |  |  |  | Choose an item. |
| DM-03(01) | Risk Minimization Techniques |  |  |  | Choose an item. |
| IP-01 | Consent |  |  |  | Choose an item. |
| IP-01(01) | Mechanisms Supporting Itemized Or Tiered Consent |  |  |  | Choose an item. |
| IP-02 | Individual Access |  |  |  | Choose an item. |
| IP-03 | Redress |  |  |  | Choose an item. |
| IP-04 | Complaint Management |  |  |  | Choose an item. |
| IP-04(01) | Response Times |  |  |  | Choose an item. |
| SE-01 | Inventory Of Personally Identifiable Information |  |  |  | Choose an item. |
| SE-02 | Privacy Incident Response |  |  |  | Choose an item. |
| TR-01 | Privacy Notice |  |  |  | Choose an item. |
| TR-01(01) | Real-Time Or Layered Notice |  |  |  | Choose an item. |
| TR-02 | System Of Records Notices And Privacy Act Statements |  |  |  | Choose an item. |
| TR-02(01) | Public Website Publication |  |  |  | Choose an item. |
| TR-03 | Dissemination Of Privacy Program Information |  |  |  | Choose an item. |
| UL-01 | Internal Use |  |  |  | Choose an item. |
| UL-02 | Information Sharing With Third Parties |  |  |  | Choose an item. |

1. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. [↑](#footnote-ref-2)