Statewide Information Technology (IT) Control Standards- Change Overview

This document provides an overview of the changes made from the 2019 Statewide Information and Cyber Security Standards to the current 2023 Statewide Information Technology (IT) Control Standards.

The first resource in this document is a two-page example of one sampled control as it was updated from the 2019 to 2023 version, and how information was incorporated from NIST, StateRAMP, and Oregon-specific needs to create the control. Within the new version, sources of the text can be seen highlighted in yellow for NIST, blue for StateRAMP, and green for Oregon-specific.

The second resource is a side-by-side spreadsheet comparison of controls that were added, removed, or maintained in the Standards. Changes in this document can be seen highlighted in blue for additions, red for removals, green for closely related and maintained, and no background/white if simply maintained.

<u>Following resources:</u>

- Standards control change example
- 2019-2023 comparison spreadsheet

Standards Control Change Example

Sample Control: AT-2

Level criteria (L, O, etc.) were removed in new standards as all controls were moved to moderate.

Previous 2019 Standards Version

AT-2 - Security Awareness Training (L, O) .

Enterprise wide

a. ***Provide all personnel (including but not limited to managers, senior executive staff, contractors, and volunteers) basic security awareness training:***
    1. ***As part of initial training for new personnel and before authorizing access to state systems, and information;***
    2. ***When required by system changes; and***
    3. ***At least annually thereafter; and***

b. ***Create a security awareness program for all personnel to complete on a regular basis to ensure understanding of the necessary behaviors and skills to help support the security of the enterprise (CIS-17.3):***
    1. ***The Security Awareness Program must be updated at least annually to address new technologies, threats, standards, and business requirements (CIS-17.4); and***
    2. ***At a minimum, training must include:***
        i. ***Information on enabling and using secure authentication (CIS-17.5);***
        ii. ***Proper identification, storage, transfer, and destruction of sensitive information (CIS-17.7);***
        iii. ***Identification of common indicators of an incident; and***
        iv. ***How to report incidents (CIS-17.9);***

c. ***All personnel with access to state information assets shall complete basic statewide security awareness training as required; and***

d. ***Provide additional training, including any training required for access to regulated data to supplement the statewide mandated awareness training.***

New 2023 Standards Version

AT-2 - ~~Literacy Training and Awareness~~ Security Awareness and Training

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 at least annually thereafter; and***
2. ***When required by system changes or following significant events;***

b. ***Employ ~~the following techniques~~ supplement training as necessary to increase the security ~~and privacy~~ awareness of system users and to meet regulatory and compliance obligations;***

c. ***Update literacy training and awareness content at least annually and following significant events; and***

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

2019 ID	2019 Control Name	2023 ID	2023 Control Name
		AC-1	Access Control Policy and Procedures
AC-2	Account Management	AC-2	Account Management
AC-2(1)	Account Management | Automated System Account Management	AC-2(1)	Account Management | Automated System Account Management
AC-2(2)	Account Management | Automated Temporary and Emergency Account Management	AC-2(2)	Account Management | Automated Temporary and Emergency Account Management
AC-2(3)	Account Management | Disable Accounts	AC-2(3)	Account Management | Disable Accounts
AC-2(4)	Account Management | Automated Audit Actions	AC-2(4)	Account Management | Automated Audit Actions
		AC-2(5)	Account Management | Inactivity Logout
		AC-2(7)	Account Management | Privileged User Accounts
		AC-2(9)	Account Management | Restrictions on Use of Shared and Group Accounts
AC-2(10)	Account Management | Shared and Group Account Credential Change		
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	AC-2(12)	Account Management | Account Monitoring for Atypical Usage
AC-2(13)	Account Management | Disable Accounts for High-risk Individuals	AC-2(13)	Account Management | Disable Accounts for High-risk Individuals
AC-3	Access Enforcement	AC-3	Access Enforcement
AC-3(7)	Access Enforcement | Role-based Access Control		
AC-4	Information Flow Enforcement	AC-4	Information Flow Enforcement
		AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows
AC-5	Separation of Duties	AC-5	Separation of Duties
AC-6	Least Privilege	AC-6	Least Privilege
AC-6(1)	Least Privilege | Authorize Access to Security Functions	AC-6(1)	Least Privilege | Authorize Access to Security Functions
AC-6(2)	Least Privilege | Non-privileged Access for Nonsecurity Functions	AC-6(2)	Least Privilege | Non-privileged Access for Nonsecurity Functions
AC-6(5)	Least Privilege | Privileged Accounts	AC-6(5)	Least Privilege | Privileged Accounts
AC-6(7)	Least Privilege | Review of User Privileges	AC-6(7)	Least Privilege | Review of User Privileges
AC-6(9)	Least Privilege | Log Use of Privileged Functions	AC-6(9)	Least Privilege | Log Use of Privileged Functions
AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions
AC-7	Unsuccessful Logon Attempts	AC-7	Unsuccessful Logon Attempts
AC-7(2)	Unsuccessful Logon Attempts | Purge or Wipe Mobile Device		
AC-8	System Use Notification	AC-8	System Use Notification
AC-11	Device Lock	AC-11	Device Lock
AC-11(1)	Device Lock | Pattern-hiding Displays	AC-11(1)	Device Lock | Pattern-hiding Displays
AC-12	Session Termination	AC-12	Session Termination
AC-14	Permitted Actions Without Identification or Authentication	AC-14	Permitted Actions Without Identification or Authentication
AC-17	Remote Access	AC-17	Remote Access
AC-17(1)	Remote Access | Monitoring and Control	AC-17(1)	Remote Access | Monitoring and Control
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	AC-17(2)	Remote Access | Protection of Confidentiality/Integrity Using Encryption
AC-17(3)	Remote Access | Managed Access Control Points	AC-17(3)	Remote Access | Managed Access Control Points
AC-17(4)	Remote Access | Privileged Commands and Access	AC-17(4)	Remote Access | Privileged Commands/Access
AC-18	Wireless Access	AC-18	Wireless Access
AC-18(1)	Wireless Access | Authentication and Encryption	AC-18(1)	Wireless Access | Authentication and Encryption
AC-18(3)	Wireless Access | Disable Wireless Networking	AC-18(3)	Wireless Access | Disable Wireless Networking
AC-19	Access Control for Mobile Devices	AC-19	Access Control for Mobile Devices
AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	AC-19(5)	Access Control for Mobile Devices | Full Device/Container-based Encryption
AC-20	Use of External Systems	AC-20	Use of External Systems
		AC-20(1)	Use of External Systems | Limits on Authorized Use
AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use	AC-20(2)	Use of External Systems | Portable Storage Devices
AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use		
		AC-21	Information Sharing
AC-22	Publicly Accessible Content	AC-22	Publicly Accessible Content
		AT-1	Awareness and Training Policy and Procedures
AT-2	Literacy Training and Awareness	AT-2	Security Awareness and Training
AT-2(2)	Literacy Training and Awareness | Insider Threat	AT-2(2)	Security Awareness and Training | Insider Threat
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	AT-2(3)	Security Awareness and Training | Social Engineering and Data Mining
AT-3	Role-based Training	AT-3	Role-based Training
AT-4	Training Records	AT-4	Security Training Records
		AU-1	Audit and Accountability Policy and Procedures
AU-2	Audit Events	AU-2	Events Logging
AU-2(3)	Audit Events | Review and Update		
AU-3	Content of Audit Records	AU-3	Content of Audit Records
AU-3(1)	Content of Audit Records | Additional Audit Information	AU-3(1)	Content of Audit Records | Additional Audit Information
AU-4	Audit Log Storage Capacity	AU-4	Audit Log Storage Capacity
AU-5	Response to Audit Logging Process Failures	AU-5	Response to Audit Processing Failures
AU-5(1)	Response to Audit Logging Process Failures | Storage Capacity Warning		
AU-6	Audit Record Review, Analysis, and Reporting	AU-6	Audit Review, Analysis, and Reporting
AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	AU-6(1)	Audit Review, Analysis, and Reporting | Process Integration
AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	AU-6(3)	Audit Review, Analysis, and Reporting | Correlate Audit Record Repositories
AU-6(4)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis		
AU-7	Audit Record Reduction and Report Generation	AU-7	Audit Record Reduction and Report Generation

2019 ID	2019 Control Name	2023 ID	2023 Control Name
AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing
AU-8	Time Stamps	AU-8	Time Stamps
AU-8(1)	Time Stamps | Synchronization With Authoritative Time Source		
AU-8(2)	Time Stamps | Secondary Authoritative Time Source		
AU-9	Protection of Audit Information	AU-9	Protection of Audit Information
AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users
AU-9(6)	Protection of Audit Information | Read-only Access		
AU-11	Audit Record Retention	AU-11	Audit Record Retention
AU-12	Audit Record Generation	AU-12	Audit Record Generation
AU-16	Cross-organizational Audit Logging		
		CA-1	Security Assessment and Authorization Policy and Procedures
CA-2	Control Assessments	CA-2	Security Assessments
CA-2(1)	Control Assessments | Independent Assessors	CA-2(1)	Control Assessments | Independent Assessors
CA-2(2)	Control Assessments | Specialized Assessments		
		CA-2(3)	Control Assessments | Leveraging Results from External Organizations
CA-3	Information Exchange	CA-3	System Interconnections
CA-3(5)	System Interconnections | Restrictions on External System Connections		
CA-5	Plan of Action and Milestones	CA-5	Plan of Action and Milestones
CA-6	Authorization	CA-6	Authorization
CA-7	Continuous Monitoring	CA-7	Continuous Monitoring
CA-7(1)	Continuous Monitoring | Independent Assessment	CA-7(1)	Continuous Monitoring | Independent Assessors
CA-7(4)	Continuous Monitoring | Risk Monitoring	CA-7(4)	Continuous Monitoring | Risk Monitoring
CA-8	Penetration Testing	CA-8	Penetration Testing
CA-8(1)	Penetration Testing | Independent Penetration Testing Agent or Team	CA-8(1)	Penetration Testing | Independent Penetration Testing Agent or Team
CA-8(2)	Penetration Testing | Red Team Exercises	CA-8(2)	Penetration Testing | Red Team Exercises
CA-8(3)	Penetration Testing | Facility Penetration Testing		
CA-9	Internal System Connections	CA-9	Internal System Connections
		CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration	CM-2	Baseline Configuration
CM-2(2)	Baseline Configuration | Automation Support for Accuracy and Currency	CM-2(2)	Baseline Configuration | Automation Support for Accuracy and Currency
CM-2(3)	Baseline Configuration | Retention of Previous Configurations	CM-2(3)	Baseline Configuration | Retention of Previous Configurations
CM-2(7)	Baseline Configuration | Configure Systems and Components for High-risk Areas	CM-2(7)	Baseline Configuration | Configure Systems and Components for High-risk Areas
CM-3	Configuration Change Control	CM-3	Configuration Change Control
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	CM-3(2)	Configuration Change Control | Test/Validate/Document Changes
CM-3(4)	Configuration Change Control | Security and Privacy Representatives	CM-3(4)	Configuration Change Control | Security Representative
CM-4	Impact Analyses	CM-4	Security Impact Analyses
CM-4(2)	Impact Analyses | Verification of Controls	CM-4(2)	Security Impact Analyses | Verification of Security Functions
CM-5	Access Restrictions for Change	CM-5	Access Restrictions for Change
		CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and Audit Records
		CM-5(5)	Access Restrictions for Change | Privilege Limitation for Production and Operation
CM-6	Configuration Settings	CM-6	Configuration Settings
		CM-6(1)	Configuration Settings | Automated Management, Application, and Verification
CM-7	Least Functionality	CM-7	Least Functionality
CM-7(1)	Least Functionality | Periodic Review	CM-7(1)	Least Functionality | Periodic Review
		CM-7(2)	Least Functionality | Prevent Program Execution
CM-7(5)	Least Functionality | Authorized Software	CM-7(5)	Least Functionality | Authorized Software - Allow by Exception
CM-8	System Component Inventory	CM-8	System Component Inventory
CM-8(1)	System Component Inventory | Updates During Installation and Removal	CM-8(1)	System Component Inventory | Updates During Installation/Removals
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection
CM-9	Configuration Management Plan	CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions	CM-10	Software Usage Restrictions
CM-10(1)	Software Usage Restrictions | Open-source Software		
CM-11	User-installed Software	CM-11	User-installed Software
CM-12	Information Location	CM-12	Information Location
CM-12(1)	Information Location | Automated Tools to Support Information Location	CM-12(1)	Information Location | Automated Tools to Support Information Location
		CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan	CP-2	Contingency Plan
CP-2(1)	Contingency Plan | Coordinate with Related Plans	CP-2(1)	Contingency Plan | Coordinate with Related Plans
CP-2(3)	Contingency Plan | Resume Mission and Business Functions	CP-2(3)	Contingency Plan | Resume Essential Mission/Business Functions
CP-2(8)	Contingency Plan | Identify Critical Assets	CP-2(8)	Contingency Plan | Identify Critical Assets
CP-3	Contingency Training	CP-3	Contingency Training
CP-4	Contingency Plan Testing	CP-4	Contingency Plan Testing
CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans	CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans
CP-6	Alternate Storage Site	CP-6	Alternate Storage Site
CP-6(1)	Alternate Storage Site | Separation from Primary Site	CP-6(1)	Alternate Storage Site | Separation from Primary Site
CP-6(3)	Alternate Storage Site | Accessibility	CP-6(3)	Alternate Storage Site | Accessibility

2019 ID	2019 Control Name	2023 ID	2023 Control Name
CP-7	Alternate Processing Site	CP-7	Alternate Processing Site
CP-7(1)	Alternate Processing Site | Separation from Primary Site	CP-7(1)	Alternate Processing Site | Separation from Primary Site
CP-7(2)	Alternate Processing Site | Accessibility	CP-7(2)	Alternate Processing Site | Accessibility
CP-7(3)	Alternate Processing Site | Priority of Service	CP-7(3)	Alternate Processing Site | Priority of Service
CP-8	Telecommunications Services	CP-8	Telecommunications Service
CP-8(1)	Telecommunications Services | Priority of Service Provisions	CP-8(1)	Telecommunications Service | Priority of Service Provisions
CP-8(2)	Telecommunications Services | Single Points of Failure	CP-8(2)	Telecommunications Service | Single Points of Failure
CP-9	System Backup	CP-9	System Backup
CP-9(1)	System Backup | Testing for Reliability and Integrity	CP-9(1)	System Backup | Testing for Reliability and Integrity
CP-9(8)	System Backup | Cryptographic Protection	CP-9(8)	System Backup | Cryptographic Protection
CP-10	System Recovery and Reconstitution	CP-10	System Recovery and Reconstruction
CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	CP-10(2)	System Recovery and Reconstruction | Transaction Recovery
		IA-1	Identification and Authorization Policy and Procedures
IA-2	Identification and Authentication (organizational Users)	IA-2	Identification and Authentication (organizational Users)
IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts
IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts
		IA-2(5)	Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication
		IA-2(6)	Identification and Authentication (organizational Users) | Access to Accounts —separate Device
IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant
		IA-2(12)	Identification and Authentication (organizational Users) | Acceptance of PIV Credentials
IA-3	Device Identification and Authentication	IA-3	Device Identification and Authentication
IA-4	Identifier Management	IA-4	Identifier Management
		IA-4(4)	Identifier Management | Identify User Status
IA-5	Authenticator Management	IA-5	Authenticator Management
IA-5(1)	Authenticator Management | Password-based Authentication	IA-5(1)	Authenticator Management | Password-based Authentication
		IA-5(2)	Authenticator Management | PKI-based Authentication
IA-5(5)	Authenticator Management | Change Authenticators Prior to Delivery		
		IA-5(6)	Authenticator Management | Protection of Authenticators
		IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators
IA-6	Authentication Feedback	IA-6	Authentication Feedback
IA-7	Cryptographic Module Authentication	IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (non-organizational Users)	IA-8	Identification and Authentication (non-organizational Users)
		IA-8(1)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies
		IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators
		IA-8(4)	Identification and Authentication (non-organizational Users) | Use of FICAM-Issued Profiles
IA-11	Re-authentication	IA-11	Identification and Authentication | Re-Authentication
IA-12	Identity Proofing	IA-12	Identity Proofing
IA-12(2)	Identity Proofing | Identity Evidence	IA-12(2)	Identity Proofing | Identity Evidence
IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification	IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification
IA-12(5)	Identity Proofing | Address Confirmation	IA-12(5)	Identity Proofing | Address Confirmation
		IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training	IR-2	Incident Response Training
IR-3	Incident Response Testing	IR-3	Incident Response Testing
IR-3(2)	Incident Response Testing | Coordination with Related Plans	IR-3(2)	Incident Response Testing | Coordination with Related Plans
IR-4	Incident Handling	IR-4	Incident Handling
IR-4(1)	Incident Handling | Automated Incident Handling Processes	IR-4(1)	Incident Handling | Automated Incident Handling Processes
IR-4(10)	Incident Handling | Supply Chain Coordination		
IR-5	Incident Monitoring	IR-5	Incident Monitoring
IR-6	Incident Reporting	IR-6	Incident Reporting
IR-6(1)	Incident Reporting | Automated Reporting	IR-6(1)	Incident Reporting | Automated Reporting
IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents		
IR-6(3)	Incident Reporting | Supply Chain Coordination	IR-6(3)	Incident Reporting | Supply Chain Coordination
IR-7	Incident Response Assistance	IR-7	Incident Response Assistance
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and Support	IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and Support
IR-7(2)	Incident Response Assistance | Coordination with External Providers		
IR-8	Incident Response Plan	IR-8	Incident Response Plan
IR-9	Information Spillage Response	IR-9	Information Spillage Response
		IR-9(2)	Information Spillage Response | Training
		IR-9(3)	Information Spillage Response | Post-spill Operations
		IR-9(4)	Information Spillage Response | Exposure to Unauthorized Personnel
		MA-1	Maintenance Policy and Procedures
MA-2	Controlled Maintenance	MA-2	Controlled Maintenance
MA-3	Maintenance Tools	MA-3	Maintenance Tools
MA-3(1)	Maintenance Tools | Inspect Tools	MA-3(1)	Maintenance Tools | Inspect Tools
MA-3(2)	Maintenance Tools | Inspect Media	MA-3(2)	Maintenance Tools | Inspect Media
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal

2019 ID	2019 Control Name	2023 ID	2023 Control Name
MA-4	Nonlocal Maintenance	MA-4	Non-local Maintenance
MA-5	Maintenance Personnel	MA-5	Maintenance Personnel
		MA-5(1)	Maintenance Personnel | Individuals Without Appropriate Access
MA-6	Timely Maintenance	MA-6	Timely Maintenance
		MP-1	Media Protection Policy and Procedures
MP-2	Media Access	MP-2	Media Access
MP-3	Media Marking	MP-3	Media Marking
MP-4	Media Storage	MP-4	Media Storage
MP-5	Media Transport	MP-5	Media Transport
MP-6	Media Sanitization	MP-6	Media Sanitization
MP-6(1)	Media Sanitization | Review, Approve, Track, Document, and Verify		
MP-7	Media Use	MP-7	Media Use
		PE-1	Physical and Environmental Protection Policy and Procedures
PE-2	Physical Access Authorizations	PE-2	Physical Access Authorizations
PE-3	Physical Access Control	PE-3	Physical Access Control
PE-4	Access Control for Transmission	PE-4	Access Control for Transmission
PE-5	Access Control for Output Devices	PE-5	Access Control for Output Devices
PE-6	Monitoring Physical Access	PE-6	Monitoring Physical Access
PE-6(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	PE-6(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment
PE-8	Visitor Access Records	PE-8	Visitor Access Records
PE-9	Power Equipment and Cabling	PE-9	Power Equipment and Cabling
PE-10	Emergency Shutoff	PE-10	Emergency Shutoff
PE-11	Emergency Power	PE-11	Emergency Power
PE-12	Emergency Lighting	PE-12	Emergency Lighting
PE-13	Fire Protection	PE-13	Fire Protection
PE-13(1)	Fire Protection | Detection Systems – Automatic Activation and Notification	PE-13(1)	Fire Protection | Detection Systems – Automatic Activation and Notification
PE-13(2)	Fire Protection | Suppression Systems – Automatic Activation and Notification	PE-13(2)	Fire Protection | Suppression Systems — Automatic Activation and Notification
PE-14	Environmental Controls	PE-14	Environmental Controls
PE-15	Water Damage Protection	PE-15	Water Damage Protection
PE-16	Delivery and Removal	PE-16	Delivery and Removal
PE-17	Alternate Work Site	PE-17	Alternate Work Site
PE-18	Location of System Components		
		PL-1	Planning Policy and Procedures
PL-2	System Security and Privacy Plans	PL-2	Security Plans
PL-2(3)	Plan / Coordinate With Other Organizational Entities		
PL-4	Rules of Behavior	PL-4	Rules of Behavior
PL-4(1)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	PL-4(1)	Rules of Behavior | Social Media and External Site/application Usage Restrictions
PL-8	Security and Privacy Architectures	PL-8	Security Architecture
PL-10	Baseline Selection	PL-10	Baseline Selection
PL-11	Baseline Tailoring	PL-11	Baseline Tailoring
PM-1	Information Security Program Plan		
PM-4	Plan of Action and Milestones Process		
PM-5	System Inventory		
		PS-1	Personnel Security Policy and Procedures
PS-2	Position Risk Designation	PS-2	Position Risk Designation
PS-3	Personnel Screening	PS-3	Personnel Screening
		PS-3(3)	Personnel Screening | Information Requiring Special Protective Measures
PS-4	Personnel Termination	PS-4	Personnel Termination
PS-5	Personnel Transfer	PS-5	Personnel Transfer
PS-6	Access Agreements	PS-6	Access Agreements
PS-7	External Personnel Security	PS-7	Third Party Personnel Security
PS-8	Personnel Sanctions	PS-8	Personnel Sanctions
		PS-9	Position Descriptions
		RA-1	Risk Assessment Policy and Procedures
RA-2	Security Categorization	RA-2	Security Categorization
RA-3	Risk Assessment	RA-3	Risk Assessment
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	RA-3(1)	Risk Assessment | Supply Chain Risk Assessment
RA-5	Vulnerability Monitoring and Scanning	RA-5	Vulnerability Monitoring and Scanning
RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	RA-5(2)	Vulnerability Monitoring and Scanning | Update by Frequency / Prior to New Scan / When Identified
		RA-5(3)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage
RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access
		RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program
RA-7	Risk Response	RA-7	Risk Response
RA-9	Criticality Analysis	RA-9	Criticality Analysis
		SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources	SA-2	Allocation of Resources

2019 ID	2019 Control Name	2023 ID	2023 Control Name
SA-3	System Development Life Cycle	SA-3	System Development Life Cycle (SDLC)
SA-4	Acquisition Process	SA-4	Acquisition Process
SA-4(1)	Acquisition Process | Functional Properties of Controls	SA-4(1)	Acquisition Process | Functional Properties of Controls
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	SA-4(2)	Acquisition Process | Design and Implementation Information for Controls
SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services in Use
		SA-4(10)	Acquisition Process | Use of Approved PIV Products
SA-5	System Documentation	SA-5	System Documentation
SA-8	Security and Privacy Engineering Principles	SA-8	Security Engineering Principles
SA-9	External System Services	SA-9	External System Services
		SA-9(1)	External System Services | Risk Assessments and Organizational Approvals
SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services
		SA-9(5)	External System Services | Processing, Storage, and Service Location
SA-10	Developer Configuration Management	SA-10	Developer Configuration Management
SA-11	Developer Testing and Evaluation	SA-11	Developer Testing and Evaluation
		SA-11(1)	Developer Testing and Evaluation | Static Code Analysis
		SA-11(2)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses
SA-12	Supply Chain Risk Management		
SA-15	Development Process, Standards, and Tools	SA-15	Development Process, Standards, and Tools
		SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis
SA-22	Unsupported System Components	SA-22	Unsupported System Components
		SC-1	System and Communications Protection Policy and Procedures
SC-2	Separation of System and User Functionality	SC-2	Separation of System and User Functionality
SC-3	Security Function Isolation		
SC-4	Information in Shared System Resources	SC-4	Information in Shared System Resources
SC-5	Denial-of-service Protection	SC-5	Denial-of-service Protection
SC-7	Boundary Protection	SC-7	Boundary Protection
SC-7(3)	Boundary Protection | Access Points	SC-7(3)	Boundary Protection | Access Points
SC-7(4)	Boundary Protection | External Telecommunications Services	SC-7(4)	Boundary Protection | External Telecommunications Services
SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	SC-7(5)	Boundary Protection | Deny by Default / Allow by Exception
SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers
SC-7(10)	Boundary Protection | Prevent Exfiltration		
SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic		
SC-7(12)	Boundary Protection | Host-based Protection	SC-7(12)	Boundary Protection | Host-based Protection
SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections		
		SC-7(18)	Boundary Protection | Fail Secure
SC-7(21)	Boundary Protection | Isolation of System Components		
SC-8	Transmission Confidentiality and Integrity	SC-8	Transmission Confidentiality and Integrity
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection
SC-10	Network Disconnect	SC-10	Network Disconnect
SC-12	Cryptographic Key Establishment and Management	SC-12	Cryptographic Key Establishment and Management
SC-13	Cryptographic Protection	SC-13	Cryptographic Protection
SC-15	Collaborative Computing Devices and Applications	SC-15	Collaborative Computing Devices and Applications
SC-17	Public Key Infrastructure Certificates	SC-17	Public Key Infrastructure Certificates
SC-18	Mobile Code	SC-18	Mobile Code
SC-18(4)	Mobile Code | Prevent Automatic Execution		
SC-19	Voice over Internet Protocol		
SC-20	Secure Name/address Resolution Service (authoritative Source)	SC-20	Secure Name/Address Resolution Service (Authoritative Source)
SC-21	Secure Name/address Resolution Service (recursive or Caching Resolver)	SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name/address Resolution Service	SC-22	Architecture and Provisioning for Name/address Resolution Service
SC-23	Session Authenticity	SC-23	Session Authenticity
SC-28	Protection of Information at Rest	SC-28	Protection of Information at Rest
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	SC-28(1)	Protection of Information at Rest | Cryptographic Protection
SC-39	Process Isolation	SC-39	Process Isolation
SC-41	Port and I/O Device Access		
		SC-45	System Time Synchronization
		SC-45(1)	System Time Synchronization | Synchronization with Authoritative Time Source
		SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation	SI-2	Flaw Remediation
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status
		SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions
SI-3	Malicious Code Protection	SI-3	Malicious Code Protection
SI-3(1)	Malicious Code Protection | Central Management		
SI-4	System Monitoring	SI-4	System Monitoring
		SI-4(1)	System Monitoring | System-wide Intrusion Detection System
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	SI-4(2)	System Monitoring | Automated Tools for Real-time Analysis

2019 ID	2019 Control Name	2023 ID	2023 Control Name
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic
SI-4(5)	System Monitoring | System-generated Alerts	SI-4(5)	System Monitoring | System-generated Alerts
SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies		
SI-4(14)	System Monitoring | Wireless Intrusion Detection		
		SI-4(16)	System Monitoring | Correlate Monitoring Information
		SI-4(18)	System Monitoring | Analyze Traffic and Covert Exfiltration
SI-4(23)	System Monitoring | Host-based Devices	SI-4(23)	System Monitoring | Host-based Devices
SI-5	Security Alerts, Advisories, and Directives	SI-5	Security Alerts, Advisories, and Directives
		SI-6	Security Function Verification
SI-7	Software, Firmware, and Information Integrity	SI-7	Software, Firmware, and Information Integrity
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response
SI-8	Spam Protection	SI-8	Spam Protection
SI-8(1)	Spam Protection | Central Management		
SI-8(2)	Spam Protection | Automatic Updates	SI-8(2)	Spam Protection | Automatic Updates
SI-10	Information Input Validation	SI-10	Information Input Validation
SI-11	Error Handling	SI-11	Error Handling
SI-12	Information Management and Retention	SI-12	Information Management and Retention
SI-16	Memory Protection	SI-16	Memory Protection
		SR-1	Supply Chain Risk Management Policy and Procedures
		SR-2	Supply Chain Risk Management Plan
		SR-2(1)	Supply Chain Risk Management Plan | Establish SCRM Team
		SR-3	Supply Chain Controls and Processes
		SR-5	Acquisition Strategies, Tools, and Methods
		SR-6	Supplier Assessments and Reviews
		SR-8	Notification Agreements
		SR-10	Inspection of Systems or Components
		SR-11	Component Authenticity
		SR-11(1)	Component Authenticity | Anti-counterfeit Training
		SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair