Information Technology (IT) System and Communications Protection (SC) Standard

February 9, 2024

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2024.02.10 16:04:44 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.0	1/14/2022	Initial draft of new standard which combines National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.
1.2	2/11/2022	Update requirements in SC-2, SC-8, and SC-28
5.3	2/9/2024	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Updated Section 4, Acronyms as appropriate. Updated language in controls SC-1, SC-4, SC-5, SC-7(7), SC-8(1) ED-03, SC-8(1) ED-04, SC-12, SC-17, and SC-28. Added controls SC-2(1), SC-3(2), SC-5(1), SC-5(2), SC-5(3), SC-7 ED-03, SC-7 ED-04, SC-7(9), SC-7(10), SC-7(11), SC-7(11) ED-01, SC-7(12), SC-7(14), SC-7(15), SC-7(17), SC-7(20), SC-7(22), SC-10 ED-01, SC-15(4), SC-18(1), SC-18(2), SC-18(4), SC-20(2), SC-23(3), SC-23(5), SC-35, SC-45, and SC-45(1). Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
2 STANDARDS 2
2.1 SC-01 Policy and Procedures (L, M, H) 3
2.2 SC-02 Separation of System and User Functionality (M, H and Control Overlay) 3
2.3 SC-03 Security Function Isolation (H) 4
2.4 SC-04 Information in Shared System Resources (M, H) 4
2.5 SC-05 Denial-of-service Protection (L, M, H) 4
2.6 SC-07 Boundary Protection (L, M, H and Control Overlay) 5
2.7 SC-08 Transmission Confidentiality and Integrity (M, H and Control Overlay) 8
2.8 SC-10 Network Disconnect (M, H) 9
2.9 SC-12 Cryptographic Key Establishment and Management (L, M, H) 9
2.10 SC-13 Cryptographic Protection (L, M, H) 10
2.11 SC-15 Collaborative Computing Devices and Applications (L, M, H) 10
2.12 SC-17 Public Key Infrastructure Certificates (M, H and Control Overlay) 10
2.13 SC-18 Mobile Code (M, H) 11
2.14 SC-20 Secure Name/Address Resolution Service (Authoritative Source) (L, M, H) 11
2.15 SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (L, M, H) 12
2.16 SC-22 Architecture and Provisioning for Name/address Resolution Service (L, M, H) 12
2.17 SC-23 Session Authenticity (M, H) 12
2.18 SC-24 Fail Known State (H) 12
2.19 SC-28 Protection of Information at Rest (M, H and Control Overlay) 12
2.20 SC-35 External Malicious Code Identification 13
2.21 SC-39 Process Isolation (L, M, H) 14
2.22 SC-45 System Time Synchronization 14
3 RISK ACCEPTANCE/POLICY EXCEPTIONS 15
4 ACRONYMS 16
APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY 18

1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) system and communications protection controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Directives, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing governance Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standard (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as amended, as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these system and communications protection control standards.

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2 STANDARDS

The Department standards for IT system and communications protection controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS PUB 199 impact-level or privacy baseline.

In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay[5] issued and maintained by the U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[6], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[7].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

Based upon an assessment of risk and determination that the level of protection for the security-relevant information within a system is not adversely impacted, media protection controls identified in the current version of NIST SP 800-53B that support only the confidentiality security objective may be downgraded to the corresponding media protection control in a lower baseline (or modified or eliminated if not defined in a lower baseline).

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

[5] HVA Control Overlay https://www.cisa.gov/resources-tools/resources/high-value-asset-control-overlay
[6] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[7] FedRAMP baselines https://www.fedramp.gov/baselines/

2.1 SC-01 Policy and Procedures (L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level IT system and communications protection policy (e.g., this document) 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.

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO is designated to manage the development, documentation, and dissemination of the Department-level IT system and communications protection policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of this policy standard and associated system and communications protection controls. The ISO and ISSO shall review system and communications protection procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 SC-02 Separation of System and User Functionality (M, H and Control Overlay)

Separate user functionality, including user interface services, from system management functionality.

[8] Also known as OCIO: 3-112

Control Overlay SC-02 ED-01 (L, M, H): Follow privileged access management principles for network-based administration of EO-critical software and EO-critical software platforms. Examples of possible implementations include using hardened platforms dedicated to administration and verified before each use.

2.2.1 SC-02(01) Separation of System and User Functionality | Interfaces for Non-Privileged Users

Prevent the presentation of system management functionality at interfaces to non-privileged users.

2.3 SC-03 Security Function Isolation (H)

Isolate security functions from nonsecurity functions.

2.3.1 SC-03(02) Security Function Isolation | Access and Flow Control Functions

Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

2.4 SC-04 Information in Shared System Resources (M, H)[9]

Prevent unauthorized and unintended information transfer via shared system resources.

2.5 SC-05 Denial-of-service Protection (L, M, H)

a. Protect against or limit the effects of the following types of denial-of-service events including, but not limited to teardrop; SYN (synchronize) flood; Smurf (internet control message protocol [ICMP]) flood; Ping flood; Ping of death; peer-to-peer attacks; and application-level floods. Refer to the current version of NIST SP 800-61, *Computer Security Incident Handling Guide*, and United States Computer Emergency Readiness Team (US-CERT) for additional guidance on the types of denial-of-service (DoS) events; and

b. Employ the following controls to achieve the denial-of-service objective: Department approved security safeguards including, but not limited to boundary protection devices; increased network capacity and bandwidth; service redundancy.

2.5.1 SC-05(01) Denial-of-service Protection | Restrict Ability to Attack Other Systems

Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: connect and transmit arbitrary information on the transport medium and use excessive system resources.

[9] SC-4 has been identified by NIST SP 800-53B as supporting only confidentiality and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported confidentiality security objective defined impact level.

2.5.2 SC-05(02) Denial-of-service Protection | Capacity, Bandwidth, and Redundancy

Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.

2.5.3 SC-05(03) Denial-of-service Protection | Detection and Monitoring

a. Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: inspection tools to detect DoS anomalies both at the perimeter of the authorization boundary as well as inside the authorization boundary on access control points that form isolation zones; and

b. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: defined system resources as required for each isolation zone based on a risk assessment.

2.6 SC-07 Boundary Protection (L, M, H and Control Overlay)

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are physically and 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.

Control Overlay SC-07 ED-01 (L, M, H): Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.

Control Overlay SC-07 ED-02 (L, M, H): Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks. Capabilities include:

a. proactively detecting threats at all layers of the stack, including the application layer, and stopping them when possible; and

b. providing the necessary information for security operations, threat hunting, incident response, and other security needs.

Control Overlay SC-07 ED-03 (L, M, H): Deploy and integrate trusted internet connection (TIC) 3.0 security objectives into the architecture of the information system:

a. Manage Traffic: connections to the information system must be filtered and logged at the network (e.g., zero trust architecture [ZTA] secure access service edge [SASE] integration) and application layer (e.g., web application firewall [WAF], proxy, application delivery controllers [ADC]).

b. Protect Traffic Confidentiality: All connections within the system must leverage approved encryption standards to protect the traffic.

c. Protect Traffic Integrity: All connections within the information system must be authenticated through approved enterprise authentication solutions (e.g., ED Identity, Credential, and Access Management [ICAM]), with the exception of documented and approved public accessible system components.

d. Ensure Service Resiliency: connections to the information system must be integrated with ZTA solutions and/or leveraging CSP native/provided availability zones and regions.

e. Ensure Effective Response: connections to the information system must provide audit log records to the ED Cyber Data Lake (EDCDL) to include the network and application layer logs.

Control Overlay SC-07 ED-04 (L, M, H): Ensure all connections at the network and application layer are submitted to CISA for collecting and aggregating security telemetry data by the National Cybersecurity Protections System (NCPS).

2.6.1 SC-07(03) Boundary Protection | Access Points (M, H)

Limit the number of external network connections to the system.

2.6.2 SC-07(04) Boundary Protection | 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 at least annually (i.e., each fiscal year) 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.

2.6.3 SC-07(05) Boundary Protection | Deny by Default — Allow by Exception (M, H)

Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces; except for Managed Trusted Internet Provider Services (MTIPS) and when all traffic is encrypted and authenticated using zero trust architectures.

2.6.4 SC-07(07) Boundary Protection | 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 Department approved security safeguards, (i.e., adequately provisioned virtual private network [VPN]).

2.6.5 SC-07(08) Boundary Protection | Route Traffic to Authenticated Proxy Servers (M, H)

Route approved and defined internal communications traffic to approved and defined external networks through authenticated proxy servers at managed interfaces.

2.6.6 SC-07(09) Boundary Protection | Restrict Threatening Outgoing Communications Traffic

a. Detect and deny outgoing communications traffic posing a threat to external systems; and

b. Audit the identity of internal users associated with denied communications.

2.6.7 SC-07(10) Boundary Protection | Prevent Exfiltration

a. Prevent the exfiltration of information; and

b. Conduct exfiltration tests at least semi-annually.

2.6.8 SC-07(11) Boundary Protection | Restrict Incoming Communications Traffic

Only allow incoming communications from documented (e.g., interconnection security agreements, service level agreements, memorandums of understanding) organization authorized sources to be routed to documented (e.g., interconnection security agreements, service level agreements, memorandums of understanding) organization authorized destinations.

Control Overlay SC-7(11) ED-01: The use of wildcards in ALLOW rules (ANY or ALL) should not be used. Default deny ANY rules with logging should be enabled.

2.6.9 SC-07(12) Boundary Protection | Host-based Protection

Implement monitored host-based boundary protection mechanisms (e.g., firewall, host-based intrusion detection system, host-based intrusion prevention system at access points and end point equipment).

2.6.10 SC-07(14) Boundary Protection | Protect Against Unauthorized Physical Connections

Protect against unauthorized physical connections at defined managed interfaces as deemed necessary in a facility physical environment risk assessment.

2.6.11 SC-07(15) Boundary Protection | Networked Privileged Accesses

Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

2.6.12 SC-07(17) Boundary Protection | Automated Enforcement of Protocol Formats

Enforce adherence to protocol formats.

2.6.13 SC-07(18) Boundary Protection | Fail Secure (H)

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

2.6.14 SC-07(20) Boundary Protection | Dynamic Isolation and Segregation

Provide the capability to dynamically isolate business/mission identified system components from other system components.

2.6.15 SC-07(21) Boundary Protection | Isolation of System Components (H)

Employ boundary protection mechanisms to isolate all information system components supporting sensitive Department mission or business functions.

2.6.16 SC-07(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains

Implement separate network addresses to connect to systems in different security domains.

2.6.17 SC-07(24) Boundary Protection | Personally Identifiable Information (P)

For systems that process personally identifiable information:

a. Apply the following processing rules to data elements of personally identifiable information: use only as authorized by the Privacy Act of 1974, the relevant System of Records Notice (SORN), and other applicable law, regulation or government-wide policy;

b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;

c. Document each processing exception; and

d. Review and remove exceptions that are no longer supported.

2.7 SC-08 Transmission Confidentiality and Integrity (M, H and Control Overlay)

Protect the confidentiality and integrity of transmitted information.

Control Overlay SC-08 ED-01 (L): Protect the confidentiality and integrity of transmitted information.

Control Overlay SC-08 ED-02 (L, M, H): Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with Executive Order 14028, *Improving the Nation's Cybersecurity* and NIST's cryptographic standards.

2.7.1 SC-08(01) Transmission Confidentiality and Integrity | Cryptographic Protection (M, H and Control Overlay)

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

Control Overlay SC-08(01) ED-01 (L, M, H): Encrypt all sensitive information (i.e., data) when in transit in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Control Overlay SC-08(01) ED-02 (L, M, H): Protect sensitive information accessed remotely with end-to-end encryption.

Control Overlay SC-08(01) ED-03 (L, M, H): Encrypt email and attachments that contain sensitive information sent to external recipients using the sender's Personal Identity Verification (PIV) card. When the capability of encrypting sensitive data for external distribution using a PIV card is not feasible, communication must be encrypted using a FIPS PUB 140-2/3 compliant version of WinZip.

Control Overlay SC-08(01) ED-04 (L, M, H): Comply with DHS Binding Operational Directive 18-01 requirements to enhance email and web security, including but not limited to enforce the use of Hypertext Transfer Protocol Secure (HTTPS), use Hypertext Transfer Protocol (HTTP) Strict Transport Security (HSTS), and remove support for known-weak cryptographic protocols and ciphers on all publicly-accessible Federal websites and web services.

2.8 SC-10 Network Disconnect (M, H)

Terminate the network connection associated with a communications session at the end of the session or after ED zero trust architecture configured parameters or networks not connected through ED SASE (e.g., VPNs) and has exceeded twelve (12) hours of inactivity.

Control Overlay SC-10 ED-01 (L): Terminate the network connection associated with a communications session at the end of the session or after ED zero trust architecture configured parameters or networks not connected through ED SASE (e.g., VPNs) and has exceeded twelve (12) hours of inactivity.

2.9 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: applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance including NIST SP 800 133R2 and FIPS PUB 140-2/3 for key generation, distribution, storage, access, and destruction.

2.9.1 SC-12(01) Cryptographic Key Establishment and Management | Availability (H)

Maintain availability of information in the event of the loss of cryptographic keys by users.

2.10 SC-13 Cryptographic Protection (L, M, H)

a. Determine the cryptographic uses including but not limited to the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals, and random number and hash generation; and

b. Implement the following types of cryptography required for each specified cryptographic use: non-deprecated FIPS-validated or National Security Agency (NSA)-approved cryptography.

2.11 SC-15 Collaborative Computing Devices and Applications (L, M, H)

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: collaborative computing devices and applications authorized for use by the Department; and

b. Provide an explicit indication of use to users physically present at the devices.

2.11.1 SC-15(04) Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants

Provide an explicit indication of current participants in collaboration meetings that involve sensitive information (e.g., federal tax return information, personally identifiable information).

2.12 SC-17 Public Key Infrastructure Certificates (M, H and Control Overlay)

a. Issue public key certificates under a Department certificate policy compliant with Federal PKI policy/trust anchor 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.

Control Overlay SC-17 ED-01 (M, H): Validate public key certificates used by the Department to the Federal PKI trust anchor for all uses, including but not limited to encryption, authentication, and authorization applications.

Control Overlay SC-17 ED-02 (M, H): Validate digital signature capabilities to the Federal Public Key Infrastructure (PKI) trust anchor and implemented in accordance with Federal PKI policy and NIST standards and guidelines.

Control Overlay SC-17 ED-03 (M, H): Use PIV credentials to validate digital signatures for all employees and contractors.

Control Overlay SC-17 ED-04 (M, H): Leverage approved Federal PKI credentials to validate digital signatures for individuals that fall outside the scope of PIV applicability.

Control Overlay SC-17 ED-05 (M, H): Ensure all devices containing sensitive information use a key recovery mechanism so that authorized personnel with legitimate need can access encrypted information.

Control Overlay SC-17 ED-06 (M, H): Prohibit use of encryption keys which are not recoverable by authorized personnel.

Control Overlay SC-17 ED-07 (M, H): Ensure requests from a non-owner of an encryption key to recover the key must be explicitly authorized by the ED Chief Information Security Officer (CISO).

2.13 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.

2.13.1 SC-18(01) Mobile Code | Identify Unacceptable Code and Take Corrective Actions

Identify unacceptable mobile code and take corrective actions (e.g., blocking, quarantine, alerting administrators).

2.13.2 SC-18(02) Mobile Code | Acquisition, Development, and Use

Verify that the acquisition, development, and use of mobile code to be deployed in the system meets all applicable security and privacy requirements.

2.13.3 SC-18(04) Mobile Code | Prevent Automatic Execution

Prevent the automatic execution of mobile code in software applications and enforce authentication and logging actions prior to executing the code.

2.14 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.

2.14.1 SC-20(02) Secure Name/Address Resolution Service (Authoritative Source) | Data Origin and Integrity

Provide data origin and integrity protection artifacts for internal name/address resolution queries.

2.15 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.

2.16 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.

2.17 SC-23 Session Authenticity (M, H)

Protect the authenticity of communications sessions.

2.17.1 SC-23(01) Session Authenticity | Invalidate Session Identifiers at Logout (Control Overlay for M, H)

Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems; control overlay applies to M, H.

Control Overlay SC-23(01) ED-01 (M, H): Invalidate session identifiers upon user logout or other session termination.

2.17.2 SC-23(03) Session Authenticity | Unique System-Generated Session Identifiers

Generate a unique session identifier for each session with system defined randomness requirements and recognize only session identifiers that are system-generated.

2.17.3 SC-23(05) Session Authenticity | Allowed Certificate Authorities

Only allow the use of agency approved certificate authorities for verification of the establishment of protected sessions.

2.18 SC-24 Fail Known State (H)

Fail to an information system-defined approved known state, as determined by ISO and ISSO for the following failures on the indicated components while preserving information system-defined state information, as determined by ISO and ISSO in failure: Information system-defined types of failures and system components, as determined by ISO and ISSO.

2.19 SC-28 Protection of Information at Rest (M, H and Control Overlay)

Protect the confidentiality and integrity of the following information at rest: all sensitive information (i.e., data) stored either on Government Furnished Equipment and Services (GFES) or non-GFES (contractor-owned) equipment including but not limited to internal or external hard

disk drives, external universal serial bus (USB) drives, shared files/folders, storage area network devices, and databases.

Control Overlay SC-28 ED-01 (L, M, H): Protect the confidentiality and integrity all sensitive information (i.e., data) at rest in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity* and NIST cryptographic standards.

Control Overlay SC-28 ED-02 (L, M, H): Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with Executive Order 14028, *Improving the Nation's Cybersecurity* and NIST cryptographic standards.

2.19.1 SC-28(01) Protection of Information at Rest | Cryptographic Protection (M, H and Control Overlay)

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on GFES or non-GFES (contractor-owned) equipment including internal or external hard disk drives, external USB drives, shared files/folders, storage area network devices, and databases for all sensitive information.

Control Overlay SC-28(01) ED-01 (L): Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on GFES or non-GFES (contractor-owned) equipment including internal or external hard disk drives, external USB drives, shared files/folders, storage area network devices, and databases for all sensitive information.

Control Overlay SC-28(01) ED-02 (L, M, H): Prohibit legacy devices that do not employ encryption capabilities (e.g., magnetic media, backup tapes, hard drives, or floppy disks) from storing sensitive information unless they are secured in Principal Office-defined, controlled environments.

Control Overlay SC-28(01) ED-03 (L, M, H): Encrypt all photocopiers, printers, fax machines, and multifunctional machines that have storage data transmission capability.

Control Overlay SC-28(01) ED-04 (L, M, H): Ensure personally owned mobile telephones, tablets, and other smart and storage devices are not used to store and access government sensitive information, unless granted a written exception from the ED CISO and managed by an approved enterprise mobile device management (MDM) solution and encryption mechanism. The MDM solution must be configured to the most restrictive settings practicable and allow for remote wipe in the event of an incident involving ED data.

2.20 SC-35 External Malicious Code Identification

Include system components that proactively seek to identify network-based malicious code or malicious websites.

2.21 SC-39 Process Isolation (L, M, H)

Maintain a separate execution domain for each executing system process.

2.22 SC-45 System Time Synchronization

Synchronize system clocks within and between systems and system components.

2.22.1 SC-45(01) System Time Synchronization | Synchronization with Authoritative Time Source

a. Compare the internal system clocks hourly with an approved authoritative time source; and

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than one second.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department Policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directive
ADC	Application Delivery Controllers
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Agency
CISO	Chief Information Security Officer
CM.AW-P	Communicate-P: Data Processing Awareness
CSF	Cybersecurity Framework
CT.DM-P	Control-P: Data Processing Management
CT.DP-P	Control-P: Disassociated Processing
DE.AE	Detect: Anomalies and Events
DE.CM	Detect: Security Continuous Monitoring
DE.DP	Detect: Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
DoS	Denial-of-Service
ED	U.S. Department of Education
EDCDL	ED Cyber Data Lake
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTI	Federal Tax Information
GFES	Government Furnished Equipment and Services
GV.MT-P	Govern-P: Monitoring and Review
GV.PO-P	Govern-P: Governance Policies, Processes, and Procedures
H	High
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVA	High Value Asset
IAS	Information Assurance Services
ICAM	Identity, Credential, and Access Management
ICMP	Internet Control Message Protocol
ID.AM	Identify: Asset Management
ID.GV	Identify: Governance
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
MDM	Mobile Device Management
MTIPS	Managed Trusted Internet Provider Services

Acronym	Definition
NCPS	National Cybersecurity Protections System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
ODP	Organization Defined Parameter
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PR.AC	Protect: Identity Management and Access Control
PR.AC-P	Protect-P: Identity Management, Authentication, and Access Control
PR.DS	Protect: Data Security
PR.DS-P	Protect-P: Data Security
PR.PT	Protect: Protective Technology
PR.PT-P	Protect-P: Protective Technology
PUB	Publication
RAF	Risk Acceptance Form
RC.IM	Recover: Improvements
Rev.	Revision
SASE	Secure Access Service Edge
SC	System and Communications Protection Family
SOAR	Security Orchestra, Automation, and Response
SORN	System of Records Notice
SP	Special Publication
SYN	Synchronize
TIC	Trusted Internet Connection
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network
WAF	Web Application Firewall
ZTA	Zero Trust Architecture

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-01	Policy and Procedures		x	x	x	DE.DP, ID.GV, GV.PO-P, GV.MT-P	DE.DP-2, GV.PO-P1, ID.GV-1, ID.GV-3, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6
SC-02	Separation of System and User Functionality			x	x	CT.DP-P	CT.DP-P3
SC-02(01)	Separation of System and User Functionality | Interfaces for Non-privileged Users					CT.DP-P	CT.DP-P3
SC-02(02)	Separation of System and User Functionality | Disassociability					CT.DP-P	CT.DP-P3
SC-03	Security Function Isolation				x	PR.AC	PR.AC-5
SC-03(01)	Security Function Isolation | Hardware Separation					PR.AC	PR.AC-5
SC-03(02)	Security Function Isolation | Access and Flow Control Functions					PR.AC	PR.AC-5
SC-03(03)	Security Function Isolation | Minimize Nonsecurity Functionality					PR.AC	PR.AC-5
SC-03(04)	Security Function Isolation | Module Coupling and Cohesiveness					PR.AC	PR.AC-5
SC-03(05)	Security Function Isolation | Layered Structures					PR.AC	PR.AC-5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-04	Information in Shared System Resources			x	x	PR.DS	PR.DS-5
SC-04(02)	Information in Shared System Resources | Multilevel or Periods Processing					PR.DS	PR.DS-5
SC-05	Denial-of-service Protection		x	x	x	PR.DS, PR.PT, DE.CM, PR.DS-P, PR.PT-P	PR.DS-4, PR.PT-4, DE.CM-1, PR.DS-P4, PR.PT-P3
SC-05(01)	Denial-of-service Protection | Restrict Ability to Attack Other Systems					PR.DS, PR.PT, DE.CM, PR.DS-P, PR.PT-P	PR.DS-4, PR.PT-4, DE.CM-1, PR.DS-P4, PR.PT-P3
SC-05(02)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy					PR.DS, PR.PT, DE.CM, PR.DS-P, PR.PT-P	PR.DS-4, PR.PT-4, DE.CM-1, PR.DS-P4, PR.PT-P3
SC-05(03)	Denial-of-service Protection | Detection and Monitoring					PR.DS, PR.PT, DE.CM, PR.DS-P, PR.PT-P	PR.DS-4, PR.PT-4, DE.CM-1, PR.DS-P4, PR.PT-P3
SC-06	Resource Availability					ID.AM, PR.PT, PR.PT-P	ID.AM-5, PR.PT-5, PR.PT-P4
SC-07	Boundary Protection		x	x	x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-07(03)	Boundary Protection | Access Points			x	x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(04)	Boundary Protection | External Telecommunications Services			x	x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(05)	Boundary Protection | Deny by Default — Allow by Exception			x	x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(07)	Boundary Protection | Split Tunneling for Remote Devices			x	x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers			x	x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-07(09)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(10)	Boundary Protection | Prevent Exfiltration					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(11)	Boundary Protection | Restrict Incoming Communications Traffic					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(12)	Boundary Protection | Host-based Protection					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-07(14)	Boundary Protection | Protect Against Unauthorized Physical Connections					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(15)	Boundary Protection | Networked Privileged Accesses					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(16)	Boundary Protection | Prevent Discovery of System Components					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(17)	Boundary Protection | Automated Enforcement of Protocol Formats					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(18)	Boundary Protection | Fail Secure				x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-07(19)	Boundary Protection | Block Communication from Non-organizationally Configured Hosts					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(20)	Boundary Protection | Dynamic Isolation and Segregation					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(21)	Boundary Protection | Isolation of System Components				x	PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(22)	Boundary Protection | Separate Subnets for Connecting to Different Security Domains					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(23)	Boundary Protection | Disable Sender Feedback on Protocol Validation Failure					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-07(24)	Boundary Protection | Personally Identifiable Information	x				PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(25)	Boundary Protection | Unclassified National Security System Connections					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(26)	Boundary Protection | Classified National Security System Connections					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(27)	Boundary Protection | Unclassified Non-national Security System Connections					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-07(28)	Boundary Protection | Connections to Public Networks					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-08	Transmission Confidentiality and Integrity			x	x	PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection			x	x	PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling					PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
SC-08(03)	Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals					PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
SC-08(04)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications					PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
SC-08(05)	Transmission Confidentiality and Integrity | Protected Distribution System					PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
SC-10	Network Disconnect			x	x	PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-5, PR.PT-4, PR.AC-P5, PR.PT-P3
SC-11	Trusted Path					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-2, PR.PT-4, PR.DS-P2, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-11(01)	Trusted Path | Irrefutable Communications Path					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-2, PR.PT-4, PR.DS-P2, PR.PT-P3
SC-12	Cryptographic Key Establishment and Management		x	x	x	PR.DS	PR.DS-1, PR.DS-2
SC-12(01)	Cryptographic Key Establishment and Management | Availability				x	PR.DS	PR.DS-1, PR.DS-2
SC-12(02)	Cryptographic Key Establishment and Management | Symmetric Keys					PR.DS	PR.DS-1, PR.DS-2
SC-12(03)	Cryptographic Key Establishment and Management | Asymmetric Keys					PR.DS	PR.DS-1, PR.DS-2
SC-12(06)	Cryptographic Key Establishment and Management | Physical Control of Keys					PR.DS	PR.DS-1, PR.DS-2
SC-13	Cryptographic Protection		x	x	x	PR.DS, PR.DS	PR.DS-1, PR.DS-2
SC-15	Collaborative Computing Devices and Applications		x	x	x	PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
SC-15(01)	Collaborative Computing Devices and Applications | Physical or Logical Disconnect					PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
SC-15(03)	Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas					PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-15(04)	Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants					PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
SC-16	Transmission of Security and Privacy Attributes					DE.AE, CT.DM-P, CM.AW-P, PR.DS-P	DE.AE-1, CT.DM-P7, CT.DM-P9, CM.AW-P6, PR.DS-P6
SC-16(01)	Transmission of Security and Privacy Attributes | Integrity Verification					DE.AE, CT.DM-P, CM.AW-P, PR.DS-P	DE.AE-1, CT.DM-P7, CT.DM-P9, CM.AW-P6, PR.DS-P6
SC-16(02)	Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms					DE.AE, CT.DM-P, CM.AW-P, PR.DS-P	DE.AE-1, CT.DM-P7, CT.DM-P9, CM.AW-P6, PR.DS-P6
SC-16(03)	Transmission of Security and Privacy Attributes | Cryptographic Binding					DE.AE, CT.DM-P, CM.AW-P, PR.DS-P	DE.AE-1, CT.DM-P7, CT.DM-P9, CM.AW-P6, PR.DS-P6
SC-17	Public Key Infrastructure Certificates			x	x	PR.AC	PR.AC-4
SC-18	Mobile Code			x	x	DE.CM	DE.CM-5
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions					DE.CM	DE.CM-5
SC-18(02)	Mobile Code | Acquisition, Development, and Use					DE.CM	DE.CM-5
SC-18(03)	Mobile Code | Prevent Downloading and Execution					DE.CM	DE.CM-5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-18(04)	Mobile Code | Prevent Automatic Execution					DE.CM	DE.CM-5
SC-18(05)	Mobile Code | Allow Execution Only in Confined Environments					DE.CM	DE.CM-5
SC-20	Secure Name/address Resolution Service (authoritative Source)		x	x	x	PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-5, PR.PT-4, PR.AC-P5, PR.PT-P3
SC-20(02)	Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity					PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-5, PR.PT-4, PR.AC-P5, PR.PT-P3
SC-21	Secure Name/address Resolution Service (recursive or Caching Resolver)		x	x	x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-22	Architecture and Provisioning for Name/address Resolution Service		x	x	x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-23	Session Authenticity			x	x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-23(01)	Session Authenticity | Invalidate Session Identifiers at Logout					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-23(03)	Session Authenticity | Unique System-generated Session Identifiers					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-23(05)	Session Authenticity | Allowed Certificate Authorities					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-24	Fail in Known State				x	RC.IM	RC.IM-2
SC-25	Thin Nodes						
SC-26	Decoys						

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-27	Platform-independent Applications						
SC-28	Protection of Information at Rest			x	x	PR.DS, PR.DS-P	PR.DS-1, PR.DS-P1
SC-28(01)	Protection of Information at Rest | Cryptographic Protection			x	x	PR.DS, PR.DS-P	PR.DS-1, PR.DS-P1
SC-28(02)	Protection of Information at Rest | Offline Storage					PR.DS, PR.DS-P	PR.DS-1, PR.DS-P1
SC-28(03)	Protection of Information at Rest | Cryptographic Keys					PR.DS, PR.DS-P	PR.DS-1, PR.DS-P1
SC-29	Heterogeneity						
SC-29(01)	Heterogeneity | Virtualization Techniques						
SC-30	Concealment and Misdirection						
SC-30(02)	Concealment and Misdirection | Randomness						
SC-30(03)	Concealment and Misdirection | Change Processing and Storage Locations						
SC-30(04)	Concealment and Misdirection | Misleading Information						
SC-30(05)	Concealment and Misdirection | Concealment of System Components						
SC-31	Covert Channel Analysis					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-31(01)	Covert Channel Analysis | Test Covert Channels for Exploitability					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-31(02)	Covert Channel Analysis | Maximum Bandwidth					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-31(03)	Covert Channel Analysis | Measure Bandwidth in Operational Environments					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-32	System Partitioning						
SC-32(01)	System Partitioning | Separate Physical Domains for Privileged Functions						
SC-34	Non-modifiable Executable Programs						
SC-34(01)	Non-modifiable Executable Programs | No Writable Storage						
SC-34(02)	Non-modifiable Executable Programs | Integrity Protection on Read-only Media						
SC-35	External Malicious Code Identification						
SC-36	Distributed Processing and Storage						
SC-36(01)	Distributed Processing and Storage | Polling Techniques						
SC-36(02)	Distributed Processing and Storage | Synchronization						
SC-37	Out-of-band Channels					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-37(01)	Out-of-band Channels | Ensure Delivery and Transmission					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-38	Operations Security					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-39	Process Isolation		x	x	x	PR.AC	PR.AC-5
SC-39(01)	Process Isolation | Hardware Separation					PR.AC	PR.AC-5
SC-39(02)	Process Isolation | Separate Execution Domain Per Thread					PR.AC	PR.AC-5
SC-40	Wireless Link Protection						
SC-40(01)	Wireless Link Protection | Electromagnetic Interference						
SC-40(02)	Wireless Link Protection | Reduce Detection Potential						
SC-40(03)	Wireless Link Protection | Imitative or Manipulative Communications Deception						
SC-40(04)	Wireless Link Protection | Signal Parameter Identification						
SC-41	Port and I/O Device Access						
SC-42	Sensor Capability and Data					CT.DP-P, CM.AW-P	CT.DP-P4, CM.AW-P1, CM.AW-P3
SC-42(01)	Sensor Capability and Data | Reporting to Authorized Individuals or Roles					CT.DP-P, CM.AW-P	CT.DP-P4, CM.AW-P1, CM.AW-P3
SC-42(02)	Sensor Capability and Data | Authorized Use					CT.DP-P, CM.AW-P	CT.DP-P4, CM.AW-P1, CM.AW-P3
SC-42(04)	Sensor Capability and Data | Notice of Collection					CT.DP-P, CM.AW-P	CT.DP-P4, CM.AW-P1, CM.AW-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SC-42(05)	Sensor Capability and Data | Collection Minimization					CT.DP-P, CM.AW-P	CT.DP-P4, CM.AW-P1, CM.AW-P3
SC-43	Usage Restrictions						
SC-44	Detonation Chambers					DE.CM	DE.CM-4, DE.CM-5
SC-45	System Time Synchronization						
SC-45(01)	System Time Synchronization | Synchronization with Authoritative Time Source						
SC-45(02)	System Time Synchronization | Secondary Authoritative Time Source						
SC-46	Cross Domain Policy Enforcement						
SC-47	Alternate Communications Paths					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-48	Sensor Relocation						
SC-48(01)	Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities						
SC-49	Hardware-enforced Separation and Policy Enforcement						
SC-50	Software-enforced Separation and Policy Enforcement						
SC-51	Hardware-based Protection						