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

February 10, 2023

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 **IAS_Governance@ed.gov**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.02.09 17:39:56 -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.

Table 1: Revision History

Version	Date	Summary of Changes
1.0	1/14/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 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
1.3	2/10/2023	Annual Review. Update broken links and add link to HVA control overlays.

Contents

INFORMATION TECHNOLOGY (IT) SYSTEM AND COMMUNICATIONS PROTECTION (SC) STANDARD 1
1 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
2 STANDARDS 1
2.1 SC-1 System and Communications Protection Policy and Procedures (L, M, H) 2
2.2 SC-2 Separation of System and User Functionality (M, H and Control Overlay) 3
2.3 SC-3 Security Function Isolation (H) 3
2.4 SC-4 Information in Shared System Resources (M, H) 3
2.5 SC-5 Denial-of-service Protection (L, M, H) 3
2.6 SC-7 Boundary Protection (L, M, H and Control Overlay) 4
2.7 SC-8 Transmission Confidentiality and Integrity (M, H and Control Overlay) 5
2.8 SC-10 Network Disconnect (M, H) 6
2.9 SC-12 Cryptographic Key Establishment and Management (L, M, H) 6
2.10 SC-13 Cryptographic Protection (L, M, H) 7
2.11 SC-15 Collaborative Computing Devices and Applications (L, M, H) 7
2.12 SC-17 Public Key Infrastructure Certificates (M, H and Control Overlay) 7
2.13 SC-18 Mobile Code (M, H) 8
2.14 SC-20 Secure Name/Address Resolution Service (Authoritative Source) (L, M, H) .. 8
2.15 SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (L, M, H) 8
2.16 SC-22 Architecture and Provisioning for Name/address Resolution Service (L, M, H) 8
2.17 SC-23 Session Authenticity (M, H) 8
2.18 SC-24 Fail Known State (H) 8
2.19 SC-28 Protection of Information at Rest (M, H and Control Overlay) 9
2.20 SC-39 Process Isolation (L, M, H) 10
3 RISK ACCEPTANCE/POLICY EXCEPTIONS 10
APPENDIX A: ACRONYMS 11
APPENDIX B: BASELINE CONTROL PARAMETER SUMMARY 12

1 INTRODUCTION

This governance document establishes Department information technology (IT) system maintenance controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. 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 regulation 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 Standards (FIPS) Publication 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 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 maintenance control standards.

2 STANDARDS

The Department standards for IT system and communications protection controls are organized to

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] [2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_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

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 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 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 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 Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

This standard directly supports the Department's integration of the NIST Cyber Security Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 SC-1 System and Communications Protection 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 OCIO: 3-112/ACSD-OCIO-004, *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 OCIO: 3-112/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,

[5] https://www.cisa.gov/publication/high-value-asset-control-overlay

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-2 Separation of System and User Functionality (M, H and Control Overlay)

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

Control Overlay SC-2 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.

2.3 SC-3 Security Function Isolation (H)

Isolate security functions from nonsecurity functions.

2.4 SC-4 Information in Shared System Resources (M, H)

Prevent unauthorized and unintended information transfer via shared system resources.

2.5 SC-5 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 flood; Smurf (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 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. etc.

2.6 SC-7 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-7 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-7 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.

2.6.1 SC-7(3) Boundary Protection | Access Points (M, H)

Limit the number of external network connections to the system.

2.6.2 SC-7(4) 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-7(5) 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-7(7) 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 VPN).

2.6.5 SC-7(8) 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-7(18) Boundary Protection | Fail Secure (H)

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

2.6.7 SC-7(21) Boundary Protection | Isolation of System Components (H)

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

2.6.8 SC-7(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-8 Transmission Confidentiality and Integrity (M, H and Control Overlay)

Protect the confidentiality and integrity of transmitted information.

Control Overlay SC-8 ED-01 (L): Protect the confidentiality and integrity of transmitted

information.

Control Overlay SC-8 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-8(1) 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-8(1) 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-8(1) ED-02 (L, M, H): Protect sensitive information accessed remotely with end-to-end encryption.

Control Overlay SC-8(1) 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 140-2/3 compliant version of WinZip.

Control Overlay SC-8(1) 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 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 zero trust architecture defined parameters; timeframes required to comply with zero trust architecture policy, standards, guidance, and memorandums from CISA, OMB, and NIST have expired; or network connectivity, including VPN and enterprise patching service communications/connectivity, has exceeded fifteen (15) hours of inactivity, unless risk accepted by the Department.

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 140-2/3 for key generation, distribution, storage, access, and destruction.

2.9.1 SC-12 (1) 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: 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.

2.12 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 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.

2.14 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.

2.15 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(1) 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(1) ED-01 (M, H): Invalidate session identifiers upon user logout or other session termination.

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 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(1) 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(1) 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(1) 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(1) ED-03 (L, M, H): Encrypt all photocopiers, printers, fax machines, and multifunctional machines that have storage data transmission capability.

Control Overlay SC-28(1) 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-39 Process Isolation (L, M, H)

Maintain a separate execution domain for each executing system process

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).

APPENDIX A: ACRONYMS

Table 2: Acronym List

ACS	Administrative Communications System
CERT	Computer Emergency Readiness Team
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
DoS	Denial of Service
ED	Department of Education
EO	Executive Order
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GFE	Government Furnished Equipment
IAS	Information Assurance Services
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PIV	Personal Identity Verification
PO	Principal Office
RAF	Risk Acceptance Form
SORN	System of Records Notices
SP	Special Publication
VPN	Virtual Private Network

APPENDIX B: BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray and notated by an asterisk.

Table 3: Summary of Baseline Controls

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-1	Policy and Procedures		x	x	x		
SC-2	Separation of System and User Functionality			x	x	CT.DP-P	CT.DP-P3
*SC-2(1)	Separation of System and User Functionality | Interfaces for Non-privileged Users					CT.DP-P	CT.DP-P3
*SC-2(2)	Separation of System and User Functionality | Disassociability					CT.DP-P	CT.DP-P3
SC-3	Security Function Isolation				x		
*SC-3(1)	Security Function Isolation | Hardware Separation						
*SC-3(2)	Security Function Isolation | Access and Flow Control Functions						
*SC-3(3)	Security Function Isolation | Minimize Nonsecurity Functionality						
*SC-3(4)	Security Function Isolation | Module Coupling and Cohesiveness						
*SC-3(5)	Security Function Isolation | Layered Structures						
SC-4	Information in Shared System Resources			x	x		
*SC-4(2)	Information in Shared System Resources | Multilevel or Periods Processing						
SC-5	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-5(1)	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-5(2)	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-5(3)	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-6	Resource Availability					ID.AM, PR.PT, PR.PT-P	ID.AM-5, PR.PT-5, PR.PT-P4
SC-7	Boundary Protection		x	x	x	PR.AC, PR.DS,	PR.AC-5, PR.DS-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
						PR.PT, DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	PR.PT-4, DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
SC-7(3)	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-7(4)	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-7(5)	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-7(7)	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-7(8)	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
*SC-7(9)	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-7(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-7(11)	Boundary Protection | Restrict Incoming Communications Traffic					PR.AC, PR.DS, PR.PT,	PR.AC-5, PR.DS-5, PR.PT-4,

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
						DE.CM, CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	DE.CM-1, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
*SC-7(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-7(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
*SC-7(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-7(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-7(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-7(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-7(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
*SC-7(19)	Boundary Protection | Block Communication from Non-organizationally Configured Hosts					PR.AC, PR.DS, PR.PT, DE.CM,	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1,

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
						CT.DM-P, PR.AC-P, PR.DS-P, PR.PT-P	CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3
*SC-7(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-7(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-7(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-7(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
SC-7(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-7(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-7(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-7(27)	Boundary Protection | Unclassified Non-national Security System Connections					PR.AC, PR.DS, PR.PT, DE.CM, CT.DM-P,	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1, CT.DM-P7,

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
						PR.AC-P, PR.DS-P, PR.PT-P	PR.AC-P5, PR.DS-P5, PR.PT-P3
*SC-7(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
*SC-7(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-8	Transmission Confidentiality and Integrity			x	x	PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection			x	x	PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
*SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling					PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
*SC-8(3)	Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals					PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
*SC-8(4)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications					PR.DS, PR.DS-P	PR.DS-2, PR.DS-P2
*SC-8(5)	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
*SC-11(1)	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		
SC-12(1)	Cryptographic Key Establishment and Management | Availability				x		
*SC-12(2)	Cryptographic Key Establishment and Management | Symmetric Keys						
*SC-12(3)	Cryptographic Key Establishment and Management | Asymmetric Keys						
*SC-12(6)	Cryptographic Key Establishment and Management | Physical Control of Keys						
SC-13	Cryptographic Protection		x	x	x		
SC-15	Collaborative Computing Devices and Applications		x	x	x	PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
*SC-15(1)	Collaborative Computing Devices and Applications | Physical or Logical Disconnect					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(3)	Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas					PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
*SC-15(4)	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(1)	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(2)	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(3)	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		
SC-18	Mobile Code			x	x	DE.CM	DE.CM-5
*SC-18(1)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions					DE.CM	DE.CM-5
*SC-18(2)	Mobile Code | Acquisition, Development, and Use					DE.CM	DE.CM-5
*SC-18(3)	Mobile Code | Prevent Downloading and Execution					DE.CM	DE.CM-5
*SC-18(4)	Mobile Code | Prevent Automatic Execution					DE.CM	DE.CM-5
*SC-18(5)	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(2)	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(1)	Session Authenticity | Invalidate Session Identifiers at Logout					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*SC-23(3)	Session Authenticity | Unique System-generated Session Identifiers					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*SC-23(5)	Session Authenticity | Allowed Certificate Authorities					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-24	Fail in Known State				x		
*SC-25	Thin Nodes						

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-26	Decoys						
*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(1)	Protection of Information at Rest | Cryptographic Protection			x	x	PR.DS, PR.DS-P	PR.DS-1, PR.DS-P1
*SC-28(2)	Protection of Information at Rest | Offline Storage					PR.DS, PR.DS-P	PR.DS-1, PR.DS-P1
*SC-28(3)	Protection of Information at Rest | Cryptographic Keys					PR.DS, PR.DS-P	PR.DS-1, PR.DS-P1
*SC-29	Heterogeneity						
*SC-29(1)	Heterogeneity | Virtualization Techniques						
*SC-30	Concealment and Misdirection						
*SC-30(2)	Concealment and Misdirection | Randomness						
*SC-30(3)	Concealment and Misdirection | Change Processing and Storage Locations						
*SC-30(4)	Concealment and Misdirection | Misleading Information						
*SC-30(5)	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(1)	Covert Channel Analysis | Test Covert Channels for Exploitability					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*SC-31(2)	Covert Channel Analysis | Maximum Bandwidth					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*SC-31(3)	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(1)	System Partitioning | Separate Physical Domains for Privileged Functions						
*SC-34	Non-modifiable Executable Programs						
*SC-34(1)	Non-modifiable Executable Programs | No Writable Storage						
*SC-34(2)	Non-modifiable Executable Programs | Integrity Protection on Read-only Media						
*SC-35	External Malicious Code Identification						
*SC-36	Distributed Processing and Storage						
*SC-36(1)	Distributed Processing and Storage | Polling Techniques						
*SC-36(2)	Distributed Processing and Storage | Synchronization						
*SC-37	Out-of-band Channels					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*SC-37(1)	Out-of-band Channels | Ensure Delivery and Transmission					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*SC-38	Operations Security					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
SC-39	Process Isolation		x	x	x		
*SC-39(1)	Process Isolation | Hardware Separation						

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-39(2)	Process Isolation | Separate Execution Domain Per Thread						
*SC-40	Wireless Link Protection						
*SC-40(1)	Wireless Link Protection | Electromagnetic Interference						
*SC-40(2)	Wireless Link Protection | Reduce Detection Potential						
*SC-40(3)	Wireless Link Protection | Imitative or Manipulative Communications Deception						
*SC-40(4)	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(1)	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(2)	Sensor Capability and Data | Authorized Use					CT.DP-P, CM.AW-P	CT.DP-P4, CM.AW-P1, CM.AW-P3
*SC-42(4)	Sensor Capability and Data | Notice of Collection					CT.DP-P, CM.AW-P	CT.DP-P4, CM.AW-P1, CM.AW-P3
*SC-42(5)	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(1)	System Time Synchronization | Synchronization with Authoritative Time Source						
*SC-45(2)	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(1)	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						