Baseline Standard

OCIO-STND-01

September 23, 2021

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
OCIO_IAS@ed.gov

Approval

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.09.23 20:35:18 -04'00'

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

Date

Revision History

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

Version	Release Date	Summary of Changes
1.0	10/15/2018	Initial draft
1.1	12/27/2019	1) Underwent FY20 Q1 policy review for accuracy and timeliness 2) Revised sections covered elsewhere by ED policy; 3) Included language in Section 3.12 requiring the creation of a Continuity Event Business Impact Analysis; and 4) Reviewed to incorporate updates to NIST SP 800-53, Rev. 4. As of December 31, 2019, that document had no updates, so no NIST updates to this document were required.
1.2	2/12/2020	CISO Review and included updated standards.
1.3	3/25/2020	Minor technical updates to Sections 3.10, 3.11, and 3.21
1.4	4/1/2020	Changed Section 3.16 to reflect that ISOs are responsible for COOP planning
1.5	6/4/2020	Section 3.11 updated to reflect current National Archives guidance on information system record retention
1.6	6/5/2020	Updated Section 3.1 to clarify guidance on PIV card usage
1.7	6/12/2020	Second revision of Section 3.11 to clarify current National Archives guidance on information system record retention
1.8	7/27/2020	Further updated Section 3.11 (Records Retention)
1.9	7/31/2020	Further updated Section 3.11 (Records Retention)
2.0	8/5/2020	Further updated Section 3.11 (Records Retention)
2.1	1/13/2021	Reviewed for accuracy and timeliness, standardized Risk Acceptance/Policy Exceptions verbiage. Updated EPMR references.
2.2	9/23/2021	Add new appendix for NIST SP 800-53, Revision 5 control parameters

Contents

1. INTRODUCTION 1

1.1. Purpose 1

1.2. Scope 1

1.3. Effective Date 1

1.4. Risk Acceptance/Policy Exceptions 1

3. STANDARDS 1

3.1. PIV Card Usage 1

3.2. Passwords 2

3.3. Encryption 2

3.4. Session Access and Lockouts 2

3.5. Physical and Environmental Security 2

3.6. Personnel Security Screening 2

3.7. Wireless and Mobile Device Security 2

3.8. Cybersecurity Awareness and Training 2

3.10. Removable Media 3

3.11. System Auditing and Accountability 3

3.12. Access Control and Authentication 4

3.13. Personnel Access 4

3.14. Rules of Behavior 4

3.15. Acceptable Use 5

3.16. Continuity of Operations (COOP) 6

3.17. Boundary Protection 6

3.18. Communications Protection 6

3.19. The Privacy Act, Privacy Impact Assessments, and System of Record Notices 7

3.20. Remote Access 8

3.21. Security Configuration Management 8

3.22. Management of Unsupported System Components 9

3.23. Information System Continuous Monitoring 10

3.24. Vulnerability and Patch Management 10

3.25. Incident Response 11

3.26. Interconnection Security Agreements 11

APPENDIX A: RESOURCES AND REFERENCES 13

APPENDIX B: NIST SP 800-53, REVISION 5 CONTROL PARAMETERS 14

1. INTRODUCTION

1.1. Purpose

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the Department of Education has established an Enterprise-wide Information Security Program (ISP) to safeguard the confidentiality, integrity, and availability of its information and systems. As part of the ISP initiative, all cybersecurity guidance developed prior to September 2018 is being replaced with a single, overarching cybersecurity policy (Directive OCIO 3-112) and supplemental Instructions and Standards.

ED Directive 3-112 superseded the Department's previous overarching cyber security policy (Handbook OCIO-01), however this document (OCIO Standard-01, or the Baseline Standard) is based on the Handbook and will remain valid until all the policies it contains have been absorbed into and superseded by supplementary Standards, at which time this Baseline Standard will be phased out.

1.2. Scope

The standards established in this document apply to all employees, contractors, and users authorized to access ED information systems; systems operated or maintained on behalf of ED; or ED information.

1.3. Effective Date

This Standard is effective as of its approval date.

1.4. 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).

3. STANDARDS

3.1. PIV Card Usage

- For **internal** users to access ED information systems, both a Personal Identity Verification (PIV) card and a Personal Identification Number (PIN) must be used.

- For **external** users (i.e., users who are not Departmental FTE or contract personnel) to access ED information systems, a NIST SP 800 63-3 analysis must be conducted prior to authorizing access to determine system role and account requirements.
- System access using just a password without a PIV card is only permitted if PIV usage is not a technically viable option, such as on legacy systems that lack PIV capability.
- If an internal user has a PIV card but it is technically infeasible for the system to utilize the PIV card for authentication, System Stakeholders must ensure that a NIST 800-63 Identity Assurance Level (IAL) / Authenticator Assurance Level (AAL) analysis is conducted to determine if Multifactor Authentication (MFA) is required.
- If MFA is required, an acceptable PIV-alternative MFA solution must be implemented and required identify-proofing must be conducted for the appropriate IAL/AAL.

3.2. Passwords

- See the **ED Password Standard** (*PR.AC: Password Parameters*) at https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.3. Encryption

- See the **ED Encryption Standard** (*PR.AC: Encryption of Computing Devices and Information*) at https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.4. Session Access and Lockouts

- See the **ED Password Standard** (*PR.AC: Password Parameters*) at https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.5. Physical and Environmental Security

- See **ED Instructions** for guidance on the impact of physical security on cyber security: https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.6. Personnel Security Screening

- See **ED Personnel Screening Standard** (*ID.GV: Contract Personnel Security Screenings*) at https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.7. Wireless and Mobile Device Security

- See the **ED Removable Media Standard** (*PR.PT: Removable Media*) at https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.8. Cybersecurity Awareness and Training

- See the **ED Cyber Security Awareness and Training Standard** (*PR.AT: Cybersecurity Awareness and Training*) at

https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.9. Cyber Risk Management Framework

- See the **ED Cyber Risk Management Framework Standard** (*Standard ID.RM: Cybersecurity Risk Management Framework*) at https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx

3.10. Removable Media

- All Principle Offices must purchase USB devices on the approved Enterprise Architecture Technology Insertion (EATI) group list or get approval from the EATI for the device prior to use.
- The USB device must be NIST FIPS 140-2 encryption compliant.
- Principle Offices are required to provide, quarterly, an inventory of the USB devices currently in use and newly purchased to the OCIO IAS and Enterprise Technology Services (ETS) for asset, and information (data) management.
- Connecting personally owned USB devices to the Department's network is prohibited
- In the event a USB device containing sensitive assets, data, or information including PII is lost or stolen, the user and any other parties aware of the loss or theft are required to immediately report the loss or theft of assets, or data, or information in accordance with the reporting requirements within Policy Instruction: *Respond*, available at https://connected.ed.gov/cybersecurity/SitePages/Instructions%20and%20Standards.aspx.

3.11. System Auditing and Accountability

Information System Owners and Information System Security Officers must ensure that user-access records and system-security audit logs are destroyed per National Archives and Record Administration (NARA) guidance on the retention of information technology operations and maintenance records, as outlined below:

- System Access Records, per NARA General Records Schedule (GRS) 3.2, Item 030, are considered temporary and may be destroyed when the business use ceases.
- Audit Logs, per NARA GRS 3.1, Item 020, must be retained for a minimum of three years, but longer retention is authorized if required for business use.
- See GRS 3.1 and GRS 3.2 for records that do not fall under the GRS descriptions outlined above.
- Verify records align to the selected GRS description.
- To verify retention requirements or for further guidance on maintenance and disposal of user-access records and system security audit logs, contact the Information Management Branch at RMHelp@ed.gov.

- Record destruction not in accordance with an approved record retention schedule is unlawful Under 44 USC 3106 and 36 CFR Part 1230, "Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records."
- Information system audit records must be reviewed and analyzed for indications of inappropriate or unusual activity
- Audit information and audit tools must be protected from unauthorized access, modification, and deletion.

3.12. Access Control and Authentication

- All Department users and devices must be identified, and their identities authenticated, before accessing the Department's systems.
- System access must be limited to (1) authorized users; (2) processes acting on behalf of authorized users; (3) authorized devices (including other systems and Government-furnished and non-Government furnished equipment); and (4) transactions and functions that authorized users are permitted to exercise.
- All access to ED systems and information must be granted following the principle of least privilege.
- The claimed identity of each user must be authenticated in such a way that the authentication is resistant to impersonation, forgery, or other misuse; and possesses strength and assurance that is commensurate with the sensitivity of the assets and information being protected.
- Department network security policies and security controls must be documented, implemented, and verified in accordance with applicable security authorization requirements to ensure that management, operational, and technical security controls are in place and operating as expected.
- Network security controls must be monitored on an ongoing basis, consistent with the Department's Cybersecurity Risk Assessment and Authorization Guide.

3.13. Personnel Access

- Personnel may not access the Department's internal network via personal or non-approved electronic devices.
- Principal Offices must ensure that assets, data, information, and information systems are protected during and after personnel actions such as terminations, separations, or transfers.
- Principal Offices must notify the Help Desk within 6 hours of personnel actions requiring the limitation or cessation of user access.
- Access for voluntarily separated employees will be terminated as soon as possible but no later than one business day after notifying the Help Desk.

3.14. Rules of Behavior

- Every General Support System and major application in the Department is required to have

specific Rules of Behavior and maintain compliance with an Acceptable Use policy. The Rules of Behavior and the Acceptable Use Policy (see section 4.11) must be system specific and defined by the ISO. At a minimum, the Rules of Behavior will:

- Inform users of their responsibilities and that they will be held accountable for their actions while accessing or administering a Department information system
- Define the consequences of noncompliance
- Inform users that they do not have any right to, or expectation of, privacy while using Department information systems, including internet and e-mail services
- Require users to accept and acknowledge the Rules of Behavior before being allowed access to any of the Department's information systems
- Include non-disclosure requirements when sensitive assets, information, and data is available for view
- Require the Principal Office to keep a record of users who have accepted and acknowledged the Rules of Behavior
- Information systems and applications must display a Department approved warning banner prior to permitting access. Only after accepting the system use notification may a user gain access to an information system or application.

3.15. Acceptable Use

- Users must comply with an Acceptable Use Policy to access Departmental assets, data, and information resources and systems when using information systems owned or controlled by other Federal departments and agencies or nonfederal governmental organizations, including when using cloud-provided services.
- Principal Offices may augment their Acceptable Use Policy to fit their needs.
- Users of the Department's IT resources must use only software that is properly licensed and registered for use at the Department.
- Users must abide by software copyright laws and not obtain, install, replicate, or use unlicensed software.
- System owners must comply with OCIO: 1-104, Personal Use of Government Equipment, to address personal use of government IT resources (equipment, e-mail, and the Internet).
- Users only may access, use, and share Department-maintained sensitive assets, data, and information to the extent it is authorized and necessary to fulfill their assigned job duties, and users must have a valid, job-related, need to know the information. The Department requires that access to controlled assets, data, and information:
    - Have a valid access authorization that is demonstrated by assigned official government duties
    - Satisfy associated personnel security criteria

- Be granted only after users have read, understood, and signed a Nondisclosure Agreement (NDA)

3.16. Continuity of Operations (COOP)

- Each Principal Office (PO) is responsible for developing (1) a Business Continuity Plan (BCP) that outlines, at the system level, a continuity of operations (COOP) strategy and estimated ability to perform essential functions during a continuity event.
- Each Information System Owner (ISO) is responsible for developing (1) a Business Impact Analysis (BIA) that outlines what impact a suspension of operations would have on the Department.
- The continuity plans for each individual information system specified as referenced by NIST SP 800-34 are constituent components of the BIA and BCP.
- The BCP Coordinator is responsible for identifying essential business functions in coordination with the Department Continuity Manager for integration with the Department COOP, as described in the Departmental Directive OM: 5-102, Continuity Program.

3.17. Boundary Protection

- All networks, based on connection type, mission needs, and risk, must incorporate adequate security controls at the network's boundary with another network.
- Boundary devices must provide sufficient levels of protection at all layers (i.e., Open System Interconnection (OSI), physical through application) to ensure the added risks are sufficiently mitigated.
- Network segregation must not impede the Department's ability to independently monitor systems, validate security configurations, identify vulnerabilities, and monitor systems and assets, and information (data) through the Department's continuous monitoring program.
- Networks or systems with external connections (i.e., internet connections) that process, store, or transmit sensitive assets, data, or information must comply with existing Federal guidance such as the Trusted Internet Connection (TIC) Reference Architecture.

3.18. Communications Protection

- All networks must ensure that communications channels are adequately protected. Protections must ensure the following, as applicable:
  - The continued confidentiality of all sensitive communications
  - The continued integrity of all communications
  - The continued availability of all communications channels
  - The continued non-repudiation of all communications
- The Department is required to use trust relationships to facilitate communications that cross network boundaries. Tools and equipment used for communications must be approved by the

appropriate Authorizing Official.

- Information systems must implement Transport Layer Security (TLS) version 1.1, at a minimum, in order to mitigate various attacks on version 1.0 of the TLS protocol. Support for TLS version 1.2 is strongly recommended.
- Servers that support Government-only applications shall be configured to support TLS 1.1, and should be configured to support TLS 1.2. These servers shall not support TLS 1.0, SSL 2.0, or SSL
- If not already supporting TLS 1.2, all Department systems must have plans in place to migrate to support TLS 1.2 as soon as possible.
- Servers that support public or business-facing applications shall be configured to support version 1.1 and should be configured to support version 1.2. These servers may also be configured to support TLS version 1.0 in order to enable interaction with citizens and businesses. These servers shall not support SSL version 3.0 or earlier. If TLS 1.0 is supported, the use of TLS 1.1 and 1.2 shall be preferred over TLS 1.0.
- Some server implementations are known to implement version negotiation incorrectly. For example, there are TLS 1.0 servers that terminate the connection when the client offers a version newer than TLS 1.0. Servers that incorrectly implement TLS version negotiation shall not be used. For additional guidance, see the most recent version of NIST Special Publication 800-52.

3.19. The Privacy Act, Privacy Impact Assessments, and System of Record Notices

- The Privacy Act of 1974, and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* requires the Department to actively identify and protect specific types of private assets, data, and information that may exist in Department systems.
- The Department's Senior Agency Official for Privacy (SAOP) and/or the Chief Privacy Officer (CPO) has the responsibility of ensuring compliance with the abovementioned guidance.
- If an Information System is determined to store, process, or transmit PII by a Privacy Threshold Analysis (PTA), then a Privacy Impact Analysis (PIA) must be conducted to determine what cybersecurity and privacy controls are needed to protect it.
- Analyses to ensure compliance must be conducted by an assigned party within the Principal Office, following OM: 6-104, and consistent with a Privacy Threshold Analysis (PTA),
- The results of the PTA and assessment will be included in the System Security Plan as part of its authorization package. The privacy assessment process is addressed in ACS Directive OFO 6-108: Privacy: Section 208 of the E-Government Act of 2002, Policy and Compliance.
- The Privacy Act also requires that any system must be declared a "System of Record" if it:
    - Contains assets, data, or information belonging to, or about individuals that is

retrieved by an individual's name or other unique identifier; or

- Contains at least one personal identifier (such as name, Social Security Number (SSN), or date of birth) by which the assets, data, or information can be retrieved.

3.20. Remote Access

- The All instances of remote access must comply with NIST SP 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*
- Users are expected to employ reasonable security measures and comply with the Department's access agreements to protect the Department's information and assets, and data, when accessing any of them remotely.

3.21. Security Configuration Management

- The Department Chief Information Security Officer (CISO) is responsible for establishing defined security baseline configuration standards and for evaluating such standards for effectiveness not less than once annually.
- The CISO acts as the authorizing authority for system configuration deviations and delegates authority to the Department Information System Security Manager (ISSM) as applicable. The Department of Education utilizes Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) as minimum-security baselines for any type of products and systems for which a STIG has been established. In addition:
    - The most updated DISA STIG on cyber security configuration management—with Department-authorized deviations as needed—is to be treated as the Department's minimum-security baseline configuration standard.
    - Until such deviations are identified and authorized, the latest established version of the DISA STIG is to be treated as the Department's secure configuration standard.
    - The Security Engineering and Architecture Branch independently verifies and validates identified recommended DISA STIG deviations and, if warranted, recommends such deviations for authorization by the Department CISO to establish Department-specific minimum-security baseline standards.
    - The authorized Department-specific minimum-security Baseline standards are maintained and published by the Security Engineering and Architecture Branch for adoption by the Department's Principal Offices.
    - In absence of a DISA STIG for a product or system, other standards can be used as a foundation for establishing the Department's Minimum-Security Baseline Standard in this order:

(1) NIST standards and baselines;

(2) other US Government standards;

(3) cyber security industry best practices, benchmarks, and guidelines (i.e. CIS.)

(3) vendors checklists and baselines;

- Each Principal Office will maintain a current inventory of systems, hardware, and software assets, and information (data) under its control throughout the respective system development lifecycles and will establish and enforce security configuration standards for information technology products employed within Department Information Systems. These security settings shall follow the Department's minimum-security baseline standards but can be more prescriptive and can supersede them with more stringent security parameters/configurations. Such security settings can also be promoted to the Department's minimum-security baseline standards through CISO authorization.
- The designated Principal Office and Project/Program Managers (P/PM) are responsible for configuration management in accordance with Department's Policies; Instructions; Standards; Processes; US Government guidelines and standards; and industry best practices, to include the establishment of single baselines and maintenance of a current and full inventory of all hardware and software configuration items.
- As part of recurring reviews, the P/PM will develop, maintain, and document applicable manual and automated processes to ensure that configuration management is enforced.
- Department ISOs, ISSOs, administrators, and users must adhere to the following policies:
    - OCIO: 1-106, *Lifecycle Management Directive Framework*, which derives its authority from OMB A-130, *Management of Federal Information Resources*;
    - OCIO: 3-110, *Software Asset Management and Acquisition Policy;*
    - Department of Education (ED) Enterprise Program Management Review (EPMR) Framework, The Enterprise Architecture Technology Insertion (EATI) Process, which can be found on the EPMR portal: https://connected.ed.gov/pm/SitePages/EPMR%20Guidance.aspx.

3.22. Management of Unsupported System Components

- The All hardware and software must be approved by the EATI for use on Department computers (laptop, desktop, server computers, and all other electronic devices) and networks.
- Hardware and software components will be verified as being approved before they may be executed or installed. A user has 30 days to seek approval or obtain a waiver for unapproved software.
- When support for components is no longer available from the developer, vendor, or manufacturer, they must be replaced unless extended support is obtained from either the component developer or third-party service supplier certified by the original component developer.
- Outdated components are subject to disapproval and removal, retirement, or acceptance of

risk.

- System owners must provide justification and documented (via a POA&M or AoR signed by the AO) approval for the continued use of unsupported system components required to satisfy mission/business needs. Exception or waiver requests are made through the Risk Acceptance Form (RAF), as documented in the Vulnerability and Patch Management section.

3.23. Information System Continuous Monitoring

- The Principal Office systems must be authorized for operation in accordance with the Department's Cybersecurity Risk Management (CRMF) Program.
- ISOs are responsible for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system and monitoring the impact of any proposed or actual changes to the system and its operational environment.
- Reports from the continuous monitoring of security controls should be provided to the AO, who uses the content of the reports when assessing system risk and making system authorization decisions.
- Systems that have been evaluated by the CISO's office as having sufficiently automated system-level continuous monitoring (as defined by the Department's *Cybersecurity Risk Assessment and Authorization Guide*.) may operate under a continuous authorization. However, Information Security Continuous Monitoring (ISCM) does not replace the security authorization requirement; rather, it supports ongoing authorization decisions. FSA systems are approved by the FSA CISO or FSA CIO.
- All Principal Offices and information systems are required to comply with the guidance specified in (1) the current version of NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*; and (2) the Department's Information Security Continuous Monitoring Roadmap, to include supplemental guidance.

3.24. Vulnerability and Patch Management

- The Principal Offices must ensure an authenticated Web Application and Data Base Application scans are conducted at a minimum in monthly basis (or as needed to be more frequent). In addition, authenticated Operating System (OS) scans are conducted at a minimum on a weekly basis. Once the Information System is integrated with the CDM program vulnerability information for all in-scope IT assets shall be updated at minimum every 72 hours.
- The Principal Offices must enforce Vulnerability and Patch management.
- Each information system must have a configuration management plan that addresses the prompt installation of patches and vulnerability remediation.
- If applicable, patches must be installed and tested on a non-production system prior to implementation on a production system. When non-production systems are not available, the

ISO with the ISSO support must identify procedures to restore the production system in the event of patch issues.

- Vulnerability remediations and Patches must be approved, within the identified timeframes, through the change management process prior to installation on systems. ISOs shall ensure the patch and remediation is implemented as soon as possible within the below set timelines based on the vulnerability criticality.
- OS Patch installation and vulnerability remediation is a function of the GSS for systems that are hosted internally by the Department. Application-level patches and vulnerability remediations are for the ISO to ensure it is completed. For systems not hosted by the Department, patches and remediations must be installed conducted in accordance with Department standard the below set timelines based on the vulnerability criticality, by the Principal Offices or its supporting contractor.
- Security patches and remediations must be installed or implemented based on risk and prioritization of resources. Deviations from patch actions the Department policies, instructions, standards, procedures, or memos must be approved and documented through the Department's RAF and an associated POA&M that will be used to track the vulnerability until it is eliminated or mitigated. Information System owners (ISO), Information System Security Officers (ISSOs), and/or other relevant system stakeholders must remediate vulnerabilities detected on externally facing systems (including High Value Assets (HVAs) and systems or assets with FIPS 199 High categorization) as follows:

  - **Critical vulnerabilities** must be remediated within **15** calendar days of initial detection.
  - **High vulnerabilities** must be remediated within **30** calendar days of initial detection.
  - **Moderate vulnerabilities** must be remediated within **90** calendar days of initial detection.
  - **Low vulnerabilities** must be remediated within **180** calendar days of initial detection.

  Note: For internally facing systems only, system stakeholders are allowed 30 days analysis before the above set timeline kicks off.

3.25. Incident Response

- All suspected security incidents, breaches, and events must be IMMEDIATELY reported to EDSOC following reporting procedures found in the Respond Instruction.
- For public and internal incident notification timelines, the Department requires that the timelines shall be as specified in the current version of NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

3.26. Interconnection Security Agreements

- All Department information systems sharing assets, information, or data must establish an Interconnection Security Agreement (ISA) when the systems are not administered by the same organization or authorized by the same AO. Additionally, ISOs must establish and document

those interconnections in accordance with Department policy.

- Networks or information systems with external connections (i.e., Internet) that process, store, or transmit sensitive assets, data, or information must comply with existing Federal guidance, such as the TIC Program Reference Architecture.

- NIST SP 800-47, *A Security Guide for Interconnection Information Technology Systems*, provides additional guidance to document information system-to-information system and information system to network interconnections.

APPENDIX A: RESOURCES AND REFERENCES

- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800

APPENDIX B: NIST SP 800-53, REVISION 5 CONTROL PARAMETERS

Parameters in this appendix reflect the minimum baseline controls for all Department systems and these requirements supersede requirements contained in all other policies, instructions, and standards.

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-1	Policy and Procedures	a. 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)]: 1. [Department-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [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]; and 2. 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].	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Information System Owner (ISO) and Information System Security Officer (ISSO) recommended prerequisites and criteria (based on defined user role(s) matrix in System Description Narrative: Types of Users) as approved Authorizing Official (AO)] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [the following attributes as defined in the user role(s) matrix in SSP System Description Narrative Template: User Types: Internal or External; Privileged (P), Non-Privileged (NP), or No Logical Access (NLA); Sensitivity Level; Authorized Privileges; and Functions Performed] for each account; e. Require approvals by [Information System Owner or assigned delegate] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Department Standards]; g. Monitor the use of accounts; h. Notify account managers and [Information System Owners, Information System Security Officers, and assigned Help Desks and support services teams, when applicable] within: 1. [As soon as possible but no later than one business day after notification received with actions for privileged users prioritized,] when accounts are no longer required; 2. [As soon as possible but no later than one business day after notification received with actions for privileged users prioritized,] when users are terminated or transferred; and 3. [As soon as possible but no later than one business day after notification received with actions for privileged users prioritized,] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Requested roles/privileges]; j. Review accounts for compliance with account management requirements [in accordance with ED Standards for user account recertification]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.		x	x	x	
AC-Access Control	AC-2(1)	Account Management | Automated System Account Management	Support the management of system accounts using [internal system functions, ED ICAM, single sign on, or recommended automated mechanisms approved by the ED AO and with email, telephonic, and text messaging notifications sent to system personnel, including the Information System Owner and Information System Security Officer, when functionality is available].			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-2(2)	Account Management | Automated Temporary and Emergency Account Management	Automatically [disables] temporary and emergency accounts after [identification that the temporary/emergency access is no longer required, not to exceed 90 days after the creation date].			x	x	
AC-Access Control	AC-2(3)	Account Management | Disable Accounts	Disable accounts within [As soon as possible but no later than one business day] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [90 days for Low and Moderate systems and 30 days for High systems and High Value Assets. If no automated capability is available, manual methods must be implemented and documented in the System Security Plan (SSP). ISSOs are responsible for ensuring inactive accounts are disabled if the system cannot do so automatically.]			x	x	
AC-Access Control	AC-2(4)	Account Management | Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.			x	x	
AC-Access Control	AC-2(5)	Account Management | Inactivity Logout	Require that users log out when [when they expect to be inactive for more than 12 hours].			x	x	
AC-Access Control	AC-2(6)	Account Management | Dynamic Privilege Management	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-2(7)	Account Management | Privileged User Accounts	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-2(8)	Account Management | Dynamic Account Management	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-2(9)	Account Management | Restrictions on Use of Shared and Group Accounts	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-2(11)	Account Management | Usage Conditions	Enforce [ED ISSO recommended circumstances and/or usage conditions which determine when system accounts can be used such as restricting usage to certain days of the week, time of day, or specific durations of time approved by the ED ISO] for [privileged user, temporary and emergency accounts].				x	
AC-Access Control	AC-2(12)	Account Management | Account Monitoring for Atypical Usage	(a) Monitor system accounts for [atypical times of day and originating IP address for a known privileged account user that are inconsistent with normal usage patterns]; and (b) Report atypical usage of system accounts to [the EDSOC and Information System Security Officer].				x	
AC-Access Control	AC-2(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [24 hours] of discovery of [a security incident reported to or under investigation by the ED Security Operation Center (EDSOC). Accounts can be directed to be disabled by CIO/CISO/ED ISSM/ISSO/ISO/COR/EDSOC in reference to a security incident. If automated disabling capability is unavailable, manual methods must be implemented and documented in the System Security Plan (SSP). ISSOs are responsible for ensuring inactive accounts are disabled.]			x	x	
AC-Access Control	AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.		x	x	x	
AC-Access Control	AC-3(3)	Access Enforcement | Mandatory Access Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(4)	Access Enforcement | Discretionary Access Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(5)	Access Enforcement | Security-relevant Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(7)	Access Enforcement | Role-based Access Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(8)	Access Enforcement | Revocation of Access Authorizations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(9)	Access Enforcement | Controlled Release	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(11)	Access Enforcement | Restrict Access to Specific Information Types	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(12)	Access Enforcement | Assert and Enforce Application Access	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(13)	Access Enforcement | Attribute-based Access Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-3(14)	Access Enforcement | Individual Access	Provide [a self service mechanism (e.g., application interface, etc.) and/or the Department's Privacy Act Request Form to enable individuals to have access to the following elements of their personally identifiable information: [those elements identified in privacy disclosures with the SAOP and OGC consulted to determine appropriate mechanisms and access rights or limitations.]	x				
AC-Access Control	AC-3(15)	Access Enforcement | Discretionary and Mandatory Access Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-4	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Web Service Security (WS Security), WS-Security Policy, WS Trust, WS Policy Framework, Security Assertion Markup Language (SAML), extensible Access Control Markup Language (XACML)].			x	x	
AC-Access Control	AC-4(1)	Information Flow Enforcement | Object Security and Privacy Attributes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(2)	Information Flow Enforcement | Processing Domains	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(4)	Information Flow Enforcement | Flow Control of Encrypted Information	Prevent encrypted information from bypassing [authorized information flow control mechanisms available for use] by [decrypting the information; blocking the flow of the encrypted information; or terminating communications sessions attempting to pass encrypted information.]				x	
AC-Access Control	AC-4(5)	Information Flow Enforcement |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Embedded Data Types						
AC-Access Control	AC-4(6)	Information Flow Enforcement | Metadata	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(7)	Information Flow Enforcement | One-way Flow Mechanisms	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(8)	Information Flow Enforcement | Security and Privacy Policy Filters	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(9)	Information Flow Enforcement | Human Reviews	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(10)	Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(11)	Information Flow Enforcement | Configuration of Security or Privacy Policy Filters	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(12)	Information Flow Enforcement | Data Type Identifiers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(13)	Information Flow Enforcement | Decomposition into Policy-relevant	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Subcomponents						
AC-Access Control	AC-4(14)	Information Flow Enforcement | Security or Privacy Policy Filter Constraints	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(15)	Information Flow Enforcement | Detection of Unsanctioned Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(17)	Information Flow Enforcement | Domain Authentication	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(19)	Information Flow Enforcement | Validation of Metadata	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(20)	Information Flow Enforcement | Approved Solutions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(22)	Information Flow Enforcement | Access Only	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-4(23)	Information Flow Enforcement | Modify Non-releasable Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(24)	Information Flow Enforcement | Internal Normalized Format	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(25)	Information Flow Enforcement | Data Sanitization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(26)	Information Flow Enforcement | Audit Filtering Actions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(27)	Information Flow Enforcement | Redundant/independent Filtering Mechanisms	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(28)	Information Flow Enforcement | Linear Filter Pipelines	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(29)	Information Flow Enforcement | Filter Orchestration Engines	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(30)	Information Flow Enforcement | Filter Mechanisms Using Multiple Processes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-4(31)	Information Flow Enforcement | Failed Content Transfer Prevention	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-4(32)	Information Flow Enforcement | Process Requirements for Information Transfer	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-5	Separation of Duties	a. Identify and document [within the system description narrative, all system user roles, the privileges and duties assigned to the role, the specific duties and privileges that the role cannot perform, and rationale for why they are incompatible]; and b. Define system access authorizations to support separation of duties.			x	x	Required for all systems, including Low security control baseline
AC-Access Control	AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.			x	x	Required for all systems, including Low security control baseline
AC-Access Control	AC-6(1)	Least Privilege | Authorize Access to Security Functions	Authorize access for [security administrators, system administrators, system security officers, system programmers, and other privileged users] to: (a) [Security functions (deployed in hardware, software, and firmware) including, at a minimum: • Establishing system accounts, configuring access authorizations (i.e., permissions, privileges); • Setting/modifying audit logs and auditing behavior; • Setting/modifying boundary protection system rules; • Configuring/modifying access authorizations (i.e., permissions, privileges); • Setting/modifying authentication parameters; and • Setting/modifying system configurations and parameters]; and (b) [filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists]			x	x	
AC-Access Control	AC-6(2)	Least Privilege | Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [security relevant information or security functions (examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions)] use non-privileged accounts or roles, when accessing nonsecurity functions.			x	x	
AC-Access Control	AC-6(3)	Least Privilege | Network Access to Privileged Commands	Authorize network access to [all privileged commands (i.e., any command requiring privileges above a standard user)] only for [compelling operational needs as approved by the Information System Owner (ISO), Information System Security Officer (ISSO), and or the Authorizing Official (AO), based upon an assessment of risk] and document the rationale for such access in the security plan for the system.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-6(4)	Least Privilege | Separate Processing Domains	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-6(5)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [individuals, services and systems/machines approved by the Information System Owner (ISO), Information System Security Officer (ISSO), and/or the Authorization Official (AO) based upon an assessment of risk].			x	x	
AC-Access Control	AC-6(6)	Least Privilege | Privileged Access by Non-organizational Users	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-6(7)	Least Privilege | Review of User Privileges	(a) Review [monthly for High Value Assets & High Impact systems and quarterly for Moderate and Low Impact systems] the privileges assigned to [all privileged roles and users] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.			x	x	
AC-Access Control	AC-6(8)	Least Privilege | Privilege Levels for Code Execution	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-6(9)	Least Privilege | Log Use of Privileged Functions	Log the execution of privileged functions.			x	x	
AC-Access Control	AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.			x	x	
AC-Access Control	AC-7	Unsuccessful Logon Attempts	a. Enforce a limit of [3] consecutive invalid logon attempts by a user during a [30-minute time period] with system accounts locked immediately upon any unsuccessful attempt to login; and b. Automatically [lock the account or node for 30 minutes, unless the user contacts the Help Desk to manually unlock the account during the 30 minute period. For system accounts and systems unable to set the 30-minute lockout duration, accounts must remain locked until being reset by an administrator. After three (3) consecutive account lock-outs due to unsuccessful login attempts, the account must be disabled until an admin can re-enable it.]		x	x	x	
AC-Access Control	AC-7(2)	Unsuccessful Logon Attempts	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		| Purge or Wipe Mobile Device						
AC-Access Control	AC-7(3)	Unsuccessful Logon Attempts | Biometric Attempt Limiting	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-7(4)	Unsuccessful Logon Attempts | Use of Alternate Authentication Factor	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-8	System Use Notification	a. Display [a system use notification message or banner approved for use by ED policy or standard] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that: 1. Users are accessing a U.S. Government system; 2. System usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4. Use of the system indicates consent to monitoring and recording; b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and c. For publicly accessible systems: 1. Display system use information [when accessed via logon interfaces with human users], before granting further access to the publicly accessible system; 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Include a description of the authorized uses of the system.		x	x	x	
AC-Access Control	AC-9	Previous Logon Notification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-9(1)	Previous Logon Notification | Unsuccessful Logons	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-9(2)	Previous Logon Notification | Successful and Unsuccessful Logons	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-9(3)	Previous Logon Notification | Notification of Account Changes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-9(4)	Previous Logon Notification | Additional Logon Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-10	Concurrent Session Control	Limit the number of concurrent sessions for each [standard user, power user, privileged user, service account and machine account] to [the number of sessions required by specific role to perform essential duties as documented and approved by the Information System Security Officer (ISSO)].				x	
AC-Access Control	AC-11	Device Lock	a. Prevent further access to the system by [initiating a device lock after 30 minutes of inactivity]; requiring the user to initiate a device lock before leaving the system unattended]; and b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.			x	x	
AC-Access Control	AC-11(1)	Device Lock | Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.			x	x	
AC-Access Control	AC-12	Session Termination	Automatically terminate a user session after [(1) zero trust architecture standards, guidance, and memorandums from CISA, OMB or NIST; (2) targeted responses to certain types of incidents; 3) time-of-day restrictions on system use, if implemented; or 4) 30 minutes of session inactivity. System-level activities, established by a virtual private network (VPN) connection, are authorized to continue after strict user interactions have ended to support remote system patching.]			x	x	
AC-Access Control	AC-12(1)	Session Termination | User-initiated Logouts	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-12(2)	Session Termination | Termination Message	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-12(3)	Session Termination | Timeout Warning Message	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-14	Permitted Actions Without Identification or Authentication	a. Identify [no user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.		x	x	x	
AC-Access Control	AC-16	Security and Privacy Attributes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(1)	Security and Privacy Attributes | Dynamic Attribute Association	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(2)	Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(3)	Security and Privacy Attributes | Maintenance of Attribute Associations by System	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(4)	Security and Privacy Attributes | Association of Attributes by Authorized Individuals	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(5)	Security and Privacy Attributes | Attribute Displays on Objects to Be Output	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(6)	Security and Privacy Attributes | Maintenance of	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Attribute Association						
AC-Access Control	AC-16(7)	Security and Privacy Attributes | Consistent Attribute Interpretation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(8)	Security and Privacy Attributes | Association Techniques and Technologies	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(9)	Security and Privacy Attributes | Attribute Reassignment — Regrading Mechanisms	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-16(10)	Security and Privacy Attributes | Attribute Configuration by Authorized Individuals	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-17	Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.		x	x	x	
AC-Access Control	AC-17(1)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.			x	x	
AC-Access Control	AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.			x	x	
AC-Access Control	AC-17(3)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AC-Access Control	AC-17(4)	Remote Access | Privileged Commands and Access	(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [ISO, ISSO, and/or AO approved special cases for remote administration and maintenance tasks]; and (b) Document the rationale for remote access in the security plan for the system.			x	x	
AC-Access Control	AC-17(6)	Remote Access | Protection of Mechanism Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-17(9)	Remote Access | Disconnect or Disable Access	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-17(10)	Remote Access | Authenticate Remote Commands	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.		x	x	x	
AC-Access Control	AC-18(1)	Wireless Access | Authentication and Encryption	Protect wireless access to the system using authentication of [users and devices] and FIPS validated encryption.			x	x	
AC-Access Control	AC-18(3)	Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.			x	x	
AC-Access Control	AC-18(4)	Wireless Access | Restrict Configurations by Users	Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.				x	
AC-Access Control	AC-18(5)	Wireless Access | Antennas and Transmission Power Levels	Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.				x	
AC-Access Control	AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.		x	x	x	
AC-Access Control	AC-19(4)	Access Control for Mobile Devices |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Restrictions for Classified Information						
AC-Access Control	AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [full device encryption whenever possible, container encryption only when full device is not possible] to protect the confidentiality and integrity of information on [ED-approved and authorized mobile devices and services].			x	x	
AC-Access Control	AC-20	Use of External Systems	a. [Establish, maintain and monitor Interconnection Security Agreements (ISAs), Inter Agency Agreements (IAA) and other agreements with external agencies per CA-3 which comply with NIST SP 800-47 and ED policy; and establish, maintain and monitor other binding agreements with employees and contractors which include ED-defined controls to be implemented on personally owned systems, components, or devices] consistent with trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [external systems not covered by a current ISA, IAA, or other agreements with external agencies per CA-3].		x	x	x	
AC-Access Control	AC-20(1)	Use of External Systems | Limits on Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: (a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or (b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.			x	x	
AC-Access Control	AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [governance policies and procedures, and when available automated technology which prohibits the use of any external system that is not ED owned or authorized including the use of personally-owned or corporate-owned systems and services].			x	x	
AC-Access Control	AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-20(4)	Use of External Systems | Network Accessible Storage Devices	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		— Prohibited Use						
AC-Access Control	AC-20(5)	Use of External Systems | Portable Storage Devices — Prohibited Use	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [information that may be restricted in some manner based on some formal or administrative determination including but not limited to contract-sensitive information, privileged information, proprietary information, and personally identifiable information]; and b. Employ [non-disclosure agreements (NDAs) and when feasible automated processes which use information flow and security attributes] to assist users in making information sharing and collaboration decisions.			x	x	
AC-Access Control	AC-21(1)	Information Sharing | Automated Decision Support	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-21(2)	Information Sharing | Information Search and Retrieval	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-22	Publicly Accessible Content	a. Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible system for nonpublic information [annually (i.e., each fiscal year)] and remove such information, if discovered.		x	x	x	
AC-Access Control	AC-23	Data Mining Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-24	Access Control Decisions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-24(1)	Access Control Decisions | Transmit Access Authorization Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AC-Access Control	AC-24(2)	Access Control Decisions | No	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		User or Process Identity						
AC-Access Control	AC-25	Reference Monitor	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AT - Awarenes s and Training	AT-1	Policy and Procedures	a. 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)]: 1. [Department-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and c. Review and update the current awareness and training: 1. Policy [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]; and 2. 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].	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AT - Awareness and Training	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [annually (i.e., each fiscal year)] thereafter; and 2. When required by system changes or following [a determination by the Department CIO, CISO, or Governance, Risk and Policy Branch (GRP) branch chief that additional training is required to manage risk]; b. Employ the following techniques to increase the security and privacy awareness of system users [conduct practical exercises that simulate actual cyber-attacks. Practical exercises may include social engineering attempts to collect information, gain unauthorized access, invoke opening malicious email attachments, or web links via spear phishing attacks]; c. Update literacy training and awareness content [annually (i.e., each fiscal year)] and following [security and privacy incidents or breaches and/or significant changes in the security environment]; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	x	x	x	x	
AT - Awareness and Training	AT-2(1)	Literacy Training and Awareness | Practical Exercises	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [annually (i.e., each fiscal year)] thereafter; and 2. When required by system changes or following [a determination by the Department CIO, CISO, or Governance, Risk and Policy Branch (GRP) branch chief that additional training is required to manage risk]; b. Employ the following techniques to increase the security and privacy awareness of system users [conduct practical exercises that simulate actual cyber-attacks. Practical exercises may include social engineering attempts to collect information, gain unauthorized access, invoke opening malicious email attachments, or web links via spear phishing attacks]; c. Update literacy training and awareness content [annually (i.e., each fiscal year)] and following [security and privacy incidents or breaches and/or significant changes in the security environment]; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.					
AT - Awareness and Training	AT-2(2)	Literacy Training and Awareness | Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat.		X	x	x	
AT - Awareness and Training	AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AT - Awareness and Training	AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AT - Awareness and Training	AT-2(5)	Literacy Training and Awareness | Advanced Persistent Threat	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AT - Awareness and Training	AT-2(6)	Literacy Training and Awareness | Cyber Threat Environment	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AT - Awareness and Training	AT-3	Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Personnel and supporting contractors with Significant Security Responsibilities (SSR)]: 1. Before authorizing access to the system, information, or performing assigned duties, and [annually (i.e., each fiscal year)] thereafter; and 2. When required by system changes; b. Update role-based training content [when new courses or curriculum is made available to the Department through existing, updated or new contracts or shared services] and following [security and privacy incidents or breaches and/or significant changes in the security environment]; and c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.	x	x	x	x	
AT - Awareness and Training	AT-3(1)	Role-based Training | Environmental Controls	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AT - Awareness and Training	AT-3(2)	Role-based Training | Physical Security Controls	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AT - Awareness and Training	AT-3(3)	Role-based Training | Practical Exercises	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AT - Awareness and Training	AT-3(5)	Role-based Training | Processing Personally Identifiable Information	Provide [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)] with initial and [annual (i.e., each fiscal year)] training in the employment and operation of personally identifiable information processing and transparency controls.	x				
AT - Awareness and Training	AT-4	Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b. Retain individual training records for [minimum three (3) years].	x	x	x	x	
AT - Awareness and Training	AT-6	Training Feedback	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-1	Policy and Procedures	a. 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)]: 1. [Department-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and c. Review and update the current audit and accountability: 1. Policy [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]; and 2. 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].	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AU - Audit and Accountability	AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [those events that are significant and relevant to the security of systems and the privacy of individuals and that provide the ability to establish, correlate, and investigate events relating to an incident or identify those responsible for one.] b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [annually (i.e., each fiscal year) or whenever there is a change in Department policies and standards, system's threat environment, or tiers and maturity model for event log management published by OMB memo].	x	x	x	x	
AU - Audit and Accountability	AU-3	Content of Audit Records	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.		x	x	x	
AU - Audit and Accountability	AU-3(1)	Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information: [as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor).]			x	x	
AU - Audit and Accountability	AU-3(3)	Content of Audit Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [authorized by the Department's SAOP].	x				
AU - Audit and Accountability	AU-4	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [reduction in the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability; at minimum audit log storage capacity must comply with Office of Management and Budget (OMB) Memorandum M-21-31 dated August 27, 2021, or successor].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AU - Audit and Accountability	AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-5	Response to Audit Logging Process Failures	a. Alert [System Administrators (Application, System, Network, etc.) and Information System Security Officer (ISSO) at a minimum] within [a matter of minutes (i.e., real-time alerts)] in the event of an audit logging process failure; and b. Take the following additional actions: [overwrite oldest audit records for those systems which are configured to offload audit logs to a separate system or shut down the information system when audit records are not offloaded to a separate system. Actions taken must comply with Office of Management and Budget (OMB) Memorandum M-21-31 dated August 27, 2021, or successor].		x	x	x	
AU - Audit and Accountability	AU-5(1)	Response to Audit Logging Process Failures | Storage Capacity Warning	Provide a warning to [System Administrators (Application, System, Network, etc.)] within [an hour] when allocated audit log storage volume reaches [75%] of repository maximum audit log storage capacity.				x	
AU - Audit and Accountability	AU-5(2)	Response to Audit Logging Process Failures | Real-time Alerts	Provide an alert within [an hour] to [System Administrators (Application, System, Network, etc.)] when the following audit failure events occur: [inability to forward audit logs to separate system, audit records overwritten, and generation of audit logs stopped].				x	
AU - Audit and Accountability	AU-5(3)	Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AU - Audit and Accountability	AU-5(4)	Response to Audit Logging Process Failures | Shutdown on Failure	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-5(5)	Response to Audit Logging Process Failures | Alternate Audit Logging Capability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-6	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor] for indications of [compromise such as unauthorized access, unauthorized account additions or role modifications, misuse of authority or access, misconfiguration, unauthorized modification or deletion of data,] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Information System Owners (ISO), Information System Security Officers (ISSOs) and ED Security Operations Control (EDSOC) personnel]; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.		x	x	x	
AU - Audit and Accountability	AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using [Unless technically unfeasible, logs must be sent to the Department Cyber Data Lake; consolidated log servers; security information event management (SIEM) system; and other Department authorized automated tools; with the ability to consolidate, analyze and report the results of audit record review as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor].			x	x	
AU - Audit and Accountability	AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.			x	x	
AU - Audit and Accountability	AU-6(4)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AU - Audit and Accountability	AU-6(5)	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	Integrate analysis of audit records with analysis of [vulnerability scanning information; performance data; system monitoring information; physical access control devices, and other systems within the system authorization boundary and/or hosting environment and other data and information as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor] to further enhance the ability to identify inappropriate or unusual activity.				x	
AU - Audit and Accountability	AU-6(6)	Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring	Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.				x	
AU - Audit and Accountability	AU-6(7)	Audit Record Review, Analysis, and Reporting | Permitted Actions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-6(8)	Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-6(9)	Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-7	Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that: a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AU - Audit and Accountability	AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure as and other content as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor].			x	x	
AU - Audit and Accountability	AU-8	Time Stamps	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet [requirements of Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.		x	x	x	
AU - Audit and Accountability	AU-9	Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Information System Owner (ISO), Information System Security Officer (ISSO), and ED Security Operations Center (EDSOC)] upon detection of unauthorized access, modification, or deletion of audit information.		x	x	x	
AU - Audit and Accountability	AU-9(1)	Protection of Audit Information | Hardware Write-once Media	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-9(2)	Protection of Audit Information | Store on Separate Physical Systems or Components	Store audit records [as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor] in a repository that is part of a physically different system or system component than the system or component being audited.				x	
AU - Audit and Accountability	AU-9(3)	Protection of Audit Information | Cryptographic Protection	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.				x	
AU - Audit and Accountability	AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only [as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor].			x	x	
AU - Audit and Accountability	AU-9(5)	Protection of Audit Information |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Dual Authorization						
AU - Audit and Accountability	AU-9(6)	Protection of Audit Information | Read-only Access	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-9(7)	Protection of Audit Information | Store on Component with Different Operating System	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-10	Non-repudiation	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [actions sufficient to prove user non-repudiation as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor].				x	
AU - Audit and Accountability	AU-10(1)	Non-repudiation | Association of Identities	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-10(2)	Non-repudiation | Validate Binding of Information Producer Identity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-10(3)	Non-repudiation | Chain of Custody	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-10(4)	Non-repudiation | Validate Binding of Information Reviewer Identity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-11	Audit Record Retention	Retain audit records for [time frames required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
AU - Audit and Accountability	AU-11(1)	Audit Record Retention | Long-term Retrieval Capability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-12	Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [all components]; b. Allow [Information System Owners and Information System Security Officers in accordance with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.		x	x	x	
AU - Audit and Accountability	AU-12(1)	Audit Record Generation | System-wide and Time-correlated Audit Trail	Compile audit records from [all components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor].				x	
AU - Audit and Accountability	AU-12(2)	Audit Record Generation | Standardized Formats	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-12(3)	Audit Record Generation | Changes by Authorized Individuals	Provide and implement the capability for [Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Owners (e.g., System Program Managers, System Project Managers)] to change the logging to be performed on [all system components] based on [change management decisions or threat criteria provided by the EDSOC and as required to comply with Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor] within [an hour].				x	
AU - Audit and Accountability	AU-12(4)	Audit Record Generation | Query Parameter Audits of Personally Identifiable Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-13	Monitoring for Information Disclosure	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-13(1)	Monitoring for Information Disclosure | Use of	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Automated Tools						
AU - Audit and Accountability	AU-13(2)	Monitoring for Information Disclosure | Review of Monitored Sites	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-13(3)	Monitoring for Information Disclosure | Unauthorized Replication of Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-14	Session Audit	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-14(1)	Session Audit | System Start-up	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-14(3)	Session Audit | Remote Viewing and Listening	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-16	Cross-organizational Audit Logging	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-16(1)	Cross-organizational Audit Logging | Identity Preservation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-16(2)	Cross-organizational Audit Logging | Sharing of Audit Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
AU - Audit and Accountability	AU-16(3)	Cross-organizational Audit Logging | Disassociability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CA - Security Assessment and Authorization	CA-1	Policy and Procedures	a. 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)]: 1. [Department-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and c. Review and update the current assessment, authorization, and monitoring: 1. Policy [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]; and 2. 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].	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CA - Security Assessment and Authorization	CA-2	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [at least annually (i.e., each fiscal year)] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Chief Information Security Officer (CISO), Authorizing Official (AO), Chief Privacy Officer/Senior Agency Official for Privacy (CPO/SAOP), Information System Owner (ISO), and Information System Security Officer (ISSO)].	x	x	x	x	
CA - Security Assessment and Authorization	CA-2(1)	Control Assessments | Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.			x	x	
CA - Security Assessment and Authorization	CA-2(2)	Control Assessments | Specialized Assessments	Include as part of control assessments, [annual (i.e., each fiscal year)], [announced], [penetration testing and other forms of security assessments to include but not be limited to the following: in-depth monitoring; malicious user testing; vulnerability scanning; insider threat assessment; performance/load testing].				x	
CA - Security Assessment and Authorization	CA-2(3)	Control Assessments | Leveraging Results from External Organizations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and Authorization	CA-3	Information Exchange	a. Approve and manage the exchange of information between the system and other systems using [interconnection security agreements (ISA); memorandum of understanding (MOU); interagency agreements (IAA); service level agreements (SLA)]; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements [at least annually (i.e., each fiscal year)].		x	x	x	Use of MTIPS for internet connectivity must be documented in ISA/MOU and CSAM Include ED NIST SP 800-47 analysis findings

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CA - Security Assessment and Authorization	CA-3(6)	Information Exchange | Transfer Authorizations	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.				x	
CA - Security Assessment and Authorization	CA-3(7)	Information Exchange | Transitive Information Exchanges	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and Authorization	CA-5	Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [monthly] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	x	x	x	x	
CA - Security Assessment and Authorization	CA-5(1)	Plan of Action and Milestones | Automation Support for Accuracy and Currency	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and Authorization	CA-6	Authorization	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by the system; and 2. Authorizes the system to operate; d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; e. Update the authorizations [in accordance with the terms and conditions established by the AO].	x	x	x	x	
CA - Security Assessment and Authorization	CA-6(1)	Authorization | Joint Authorization — Intra-organization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and	CA-6(2)	Authorization | Joint Authorization — Inter-organization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Authorization								
CA - Security Assessment and Authorization	CA-7	Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: [metrics as defined in the latest version of the IAS ISCM Roadmap]; b. Establishing [at least monthly] for monitoring and [annually (i.e., each fiscal year)] for assessment of control effectiveness [or in accordance with Ongoing Security Authorization assessment schedule and in conjunction with the Organizational CDM Program]; c. Ongoing control assessments in accordance with the continuous monitoring strategy; d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e. Correlation and analysis of information generated by control assessments and monitoring; f. Response actions to address results of the analysis of control assessment and monitoring information; and g. Reporting the security and privacy status of the system to [CISO, AO, CPO/SAOP] [monthly].	x	x	x	x	
CA - Security Assessment and Authorization	CA-7(1)	Continuous Monitoring | Independent Assessment	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.			x	x	
CA - Security Assessment and Authorization	CA-7(3)	Continuous Monitoring | Trend Analyses	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and Authorization	CA-7(4)	Continuous Monitoring | Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following: (a) Effectiveness monitoring; (b) Compliance monitoring; and (c) Change monitoring.	x	x	x	x	
CA - Security Assessment and Authorization	CA-7(5)	Continuous Monitoring | Consistency Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CA - Security Assessment and Authorization	CA-7(6)	Continuous Monitoring | Automation Support for Monitoring	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and Authorization	CA-8	Penetration Testing	Conduct penetration testing [at least annually (i.e., each fiscal year)] on [all FIPS 199 High impact and High Value Asset (HVA) information systems].				x	
CA - Security Assessment and Authorization	CA-8(1)	Penetration Testing | Independent Penetration Testing Agent or Team	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.				x	
CA - Security Assessment and Authorization	CA-8(2)	Penetration Testing | Red Team Exercises	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and Authorization	CA-8(3)	Penetration Testing | Facility Penetration Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CA - Security Assessment and Authorization	CA-9	Internal System Connections	a. Authorize internal connections of [all components or classes of components] to the system; b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; c. Terminate internal system connections after [15 minutes of inactivity for non-persistent connections]; and d. Review [at least annually (i.e., each fiscal year)] the continued need for each internal connection.		x	x	x	
CA - Security Assessment and Authorization	CA-9(1)	Internal System Connections | Compliance Checks	Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CM - Configuration Management	CM-1	Policy and Procedures	a. 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)]: 1. [Department-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate a [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and c. Review and update the current configuration management: 1. Policy [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]; and 2. 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].	x	x	x	x	
CM - Configuration Management	CM-2	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [At a minimum annually (i.e., each fiscal year)]; 2. When required due to [significant system change]; and 3. When system components are installed or upgraded.		x	x	x	
CM - Configuration Management	CM-2(2)	Baseline Configuration | Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [applicable manual and automated tools designated by the PO and approved for use by the EA(TI)].			x	x	
CM - Configuration Management	CM-2(3)	Baseline Configuration | Retention of Previous Configurations	Retain [at a minimum one (1)] of previous versions of baseline configurations of the system to support rollback.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CM - Configuration Management	CM-2(6)	Baseline Configuration | Development and Test Environments	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-2(7)	Baseline Configuration | Configure Systems and Components for High-risk Areas	(a) Issue [ED approved foreign travel device to include but not limited to: ED-provided services, ED-issued laptops, smartphones, USB Flash drives, Personal Data Assistants (PDA), external hard drive, or any other mobile devices that store, transmit, receive, or process information] with [ED approved security safeguards, to include but not limited to: software and/or hardware configuration and security settings as defined in the Standard PR.IP: International Travel and use of Education IT Services] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Apply the following controls to the systems or components when the individuals return from travel: [examination for signs of tampering, reimaging of the hard drive (MP), scanning for malware (RA-5) as defined in the Standard PR.IP: International Travel and use of Education IT Services].			x	x	
CM - Configuration Management	CM-3	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [a minimum of 6 months]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [the ED Configuration Change Board (CCB) or CCB approved alternate] that convenes [at a minimum monthly or in accordance with ED CCB process documentation].			x	x	
CM - Configuration Management	CM-3(1)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	Use [ED approved automated mechanisms] to: (a) Document proposed changes to the system; (b) Notify [ED Configuration Change Board (CCB), Information System Owner (ISO), and Information System Security Officer (ISSO)] of proposed changes to the system and request change approval; (c) Highlight proposed changes to the system that have not been approved or disapproved within [time period specified in the change management process documentation]; (d) Prohibit changes to the system until designated approvals are received; (e) Document all changes to the system; and (f) Notify [ED Configuration Change Board (CCB), Information System Owner (ISO), and Information System Security Officer (ISSO)] when approved changes to the system are completed.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CM - Configuration Management	CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.			x	x	
CM - Configuration Management	CM-3(3)	Configuration Change Control | Automated Change Implementation	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [ED approved automated mechanisms].					
CM - Configuration Management	CM-3(4)	Configuration Change Control | Security and Privacy Representatives	Require [ED required security and privacy representatives] to be members of the [CCB].			x	x	
CM - Configuration Management	CM-3(5)	Configuration Change Control | Automated Security Response	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-3(6)	Configuration Change Control | Cryptography Management	Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [to include but not limited to: data encryption (at rest and in transit); PKI usage; device encryption; websites and web services; email server security]				x	
CM - Configuration Management	CM-3(7)	Configuration Change Control | Review System Changes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-4	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	x	x	x	x	
CM - Configuration	CM-4(1)	Impact Analyses |	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Management		Separate Test Environments						
CM - Configuration Management	CM-4(2)	Impact Analyses | Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.			x	x	
CM - Configuration Management	CM-5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.		x	x	x	
CM - Configuration Management	CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	(a) Enforce access restrictions using [ED approved automated mechanisms]; and (b) Automatically generate audit records of the enforcement actions.				x	
CM - Configuration Management	CM-5(4)	Access Restrictions for Change | Dual Authorization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-5(5)	Access Restrictions for Change | Privilege Limitation for Production and Operation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-5(6)	Access Restrictions for Change | Limit Library Privileges	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CM - Configuration Management	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [DISA STIGs, USGCB technical guidelines, NIST SP 800-70, Center for Internet Security (CIS) guidelines, vendor checklists and baselines, and/or industry best practice guidelines, as reviewed and accepted by the Department]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [individual components within systems including, but not limited to, servers, workstations, network components and databases] based on [explicit operational requirements which are documented in the information system SSP and/or Secure Configuration Baseline]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.		x	x	x	
CM - Configuration Management	CM-6(1)	Configuration Settings | Automated Management, Application, and Verification	Manage, apply, and verify configuration settings for [key components of infrastructure, to include but not limited to: network servers, desktops and databases related to those information systems based on mission requirements running within the FISMA system boundary] using [ED approved automated mechanisms].				x	
CM - Configuration Management	CM-6(2)	Configuration Settings | Respond to Unauthorized Changes	Take the following actions in response to unauthorized changes to [approved baseline configuration settings]: [alert designated organizational personnel including the EDSOC, ISO, ISSO; restore established configuration settings, or in extreme cases, halt affected information system processing].				x	
CM - Configuration Management	CM-7	Least Functionality	a. Configure the system to provide only [mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [not needed to conduct business as specified in ED minimum security baselines (e.g., HTTP, Telnet, FTP); DISA STIGs; NIST standards and baselines; other US Government standards; cyber security industry best practices, benchmarks, and guidelines; and vendor checklists and baselines, as determined to be appropriate by the CISO].		x	x	x	Maintenance Ports (MA-4) shall be disabled when not in use Additional ED specific insecure ports, protocol, service guidance
CM - Configuration Management	CM-7(1)	Least Functionality | Periodic Review	(a) Review the system [at a minimum annually (i.e., each fiscal year) for non-HVA systems, quarterly for HVA] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [unnecessary and/or non secure functions, ports, protocols, and services as authorized by the CISO.]			x	x	
CM - Configuration Management	CM-7(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [ED defined policies regarding software program usage and restrictions, to include but not limited to ED authorized software programs (i.e., allow-list) and only in circumstances where it is technologically infeasible to deploy and operate allow-list will deny-list be permitted			x	x	ED specific policy related to the Email protocols (and services) shall be configured to implement least functionality principles.

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CM - Configuration Management	CM-7(3)	Least Functionality | Registration Compliance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-7(4)	Least Functionality | Unauthorized Software	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-7(5)	Least Functionality | Authorized Software	(a) Identify [software programs authorized to execute on ED information systems]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs [at a minimum annually (i.e., each fiscal year)].			x	x	
CM - Configuration Management	CM-7(6)	Least Functionality | Confined Environments with Limited Privileges	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-7(7)	Least Functionality | Code Execution in Protected Environments	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-7(8)	Least Functionality | Binary or Machine Executable Code	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-7(9)	Least Functionality | Prohibiting The Use of Unauthorized Hardware	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CM - Configuration Management	CM-8	System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: [As defined in CSAM System Information: Appendix S - Hardware Listing and System Information: Appendix T - Software Listing]; and b. Review and update the system component inventory [at a minimum quarterly].		x	x	x	
CM - Configuration Management	CM-8(1)	System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.			x	x	Include LOW security control baseline systems. All Department technology-based information systems must be registered in CSAM.
CM - Configuration Management	CM-8(2)	System Component Inventory | Automated Maintenance	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [the Department's system of record for system inventory].				x	
CM - Configuration Management	CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [ISO-defined mechanisms used for continuous monitoring as defined in the OCIO: 3-110/ACSD-OCIO-011 (Software Asset Management Acquisition Policy)] [Continuously/ongoing basis]; and (b) Take the following actions when unauthorized components are detected: [isolate the components, notify the Information System Security Officer (ISSO) The ISSO will notify the EARB as defined in OCIO: 3-110/ACSD-OCIO-011 (Software Asset Management Acquisition Policy)]			x	x	
CM - Configuration Management	CM-8(4)	System Component Inventory | Accountability Information	Include in the system component inventory information, a means for identifying by [name, Principal Office (PO), position, and role], individuals responsible and accountable for administering those components.				x	
CM - Configuration Management	CM-8(6)	System Component Inventory | Assessed Configurations and Approved Deviations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration	CM-8(7)	System Component Inventory |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Management		Centralized Repository						
CM - Configuration Management	CM-8(8)	System Component Inventory | Automated Location Tracking	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-8(9)	System Component Inventory | Assignment of Components to Systems	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-9	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management; d. Is reviewed and approved by [Information System Owner (ISO) and Information System Security Officer (ISSO)]; and e. Protects the configuration management plan from unauthorized disclosure and modification.			x	x	
CM - Configuration Management	CM-9(1)	Configuration Management Plan | Assignment of Responsibility	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		x	x	x	
CM - Configuration Management	CM-10(1)	Software Usage Restrictions | Open-source Software	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CM - Configuration Management	CM-11	User-installed Software	a. Establish [policies as specified in OCIO: 3-110/ACSD-OCIO-011 (Software Asset Management Acquisition Policy) and ED Acceptable Use] governing the installation of software by users; b. Enforce software installation policies through the following methods:[automated and manual methods for the continuous monitoring of ED information systems.]; and c. Monitor policy compliance [through the continuous monitoring process].		x	x	x	
CM - Configuration Management	CM-11(2)	User-installed Software | Software Installation with Privileged Status	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-11(3)	User-installed Software | Automated Enforcement and Monitoring	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-12	Information Location	a. Identify and document the location of [Personally Identifiable Information (PII); Payment Card Industry (PCI) data; Identity, Credentialing, and Access Management (ICAM) data (includes but is not limited to identifier and authenticator data such as passwords, tokens, keys, certificates, hashes); system- and application-security log data; and, other sensitive data as determined by the CISO or CPO/SAOP] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.			x	x	
CM - Configuration Management	CM-12(1)	Information Location | Automated Tools to Support Information Location	Use automated tools to identify [Personally Identifiable Information (PII); Payment Card Industry (PCI) data; Identity, Credentialing, and Access Management (ICAM) data (includes but is not limited to identifier and authenticator data such as passwords, tokens, keys, certificates, hashes); system- and application-security log data; and, other sensitive data as determined by the CISO or CPO/SAOP] on [all system components for FIPS 199 Moderate and High impact information systems, HVA information systems, and networks or information systems with external connections that process, store, or transmit sensitive data or information.] to ensure controls are in place to protect organizational information and individual privacy.			x	x	DLP MS 0365 Requirements
CM - Configuration Management	CM-13	Data Action Mapping	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CM - Configuration Management	CM-14	Signed Components	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-1	Policy and Procedures	a. 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)]: 1. [Department-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls; b. Designate an [Department Chief Information Security Officer (CISO)] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and c. Review and update the current contingency planning: 1. Policy [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]; and 2. 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].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-2	Contingency Plan	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by [Information System Owner (ISO) and the Information System Security Officer (ISSO)]; b. Distribute copies of the contingency plan to [key contingency personnel, to include all response team personnel such as Telecommunications team]; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the system [annually]; e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to [Information System Security Officer (ISSO), Information System Owner (ISO), and other key contingency personnel.]; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; h. Protect the contingency plan from unauthorized disclosure and modification; and		x	x	x	
CP - Contingency Planning	CP-2(1)	Contingency Plan | Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.			x	x	
CP - Contingency Planning	CP-2(2)	Contingency Plan | Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.				x	
CP - Contingency Planning	CP-2(3)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [mission essential functions (MEF), national essential functions (NEF), and] mission and business functions within [system-level specified timeframes and metrics defined in the information system contingency plan (ISCP) and Business Impact Analysis (BIA)] of contingency plan activation.			x	x	
CP - Contingency Planning	CP-2(5)	Contingency Plan | Continue Mission and Business Functions	Plan for the continuance of [mission essential functions, as documented within the Department Continuity of Operations Plan (COOP),] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-2(6)	Contingency Plan | Alternate Processing and Storage Sites	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-2(7)	Contingency Plan | Coordinate with External Service Providers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-2(8)	Contingency Plan | Identify Critical Assets	Identify critical system assets supporting [critical and essential] mission and business functions, as documented within the Department Continuity of Operations Plan (COOP).			x	x	
CP - Contingency Planning	CP-3	Contingency Training	a. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. Within [thirty (30) days] of assuming a contingency role or responsibility; 2. When required by system changes; and 3. [annually (i.e., each fiscal year)] thereafter; and b. Review and update contingency training content [annually (i.e., each fiscal year)] and following [events to include but not limited to contingency plan test, lessons learned, assessment or audit findings, security incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines].		x	x	x	
CP - Contingency Planning	CP-3(1)	Contingency Training | Simulated Events	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.				x	
CP - Contingency Planning	CP-3(2)	Contingency Training | Mechanisms Used in Training Environments	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-4	Contingency Plan Testing	a. Test the contingency plan for the system [at least annually and following major system changes] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Low-impact system: conduct annual tabletop exercise; Moderate-impact system: conduct annual functional exercise; and High-impact systems conduct full-scale functional exercise to include system failover to the alternate location.] b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.		x	x	x	
CP - Contingency Planning	CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans.			x	x	
CP - Contingency Planning	CP-4(2)	Contingency Plan Testing | Alternate Processing Site	Test the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations.				x	
CP - Contingency Planning	CP-4(3)	Contingency Plan Testing | Automated Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-4(4)	Contingency Plan Testing | Full Recovery and Reconstitution	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-4(5)	Contingency Plan Testing | Self-challenge	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-6	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.			x	x	
CP - Contingency Planning	CP-6(1)	Alternate Storage Site | Separation from Primary Site	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.			x	x	
CP - Contingency Planning	CP-6(2)	Alternate Storage Site | Recovery Time and Recovery Point Objectives	Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.				x	
CP - Contingency Planning	CP-6(3)	Alternate Storage Site | Accessibility	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.			x	x	
CP - Contingency Planning	CP-7	Alternate Processing Site	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [information system operations] for essential mission and business functions within [the time period defined in the system-specific ISCP] when the primary processing capabilities are unavailable; b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and c. Provide controls at the alternate processing site that are equivalent to those at the primary site.			x	x	
CP - Contingency Planning	CP-7(1)	Alternate Processing Site | Separation from Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.			x	x	
CP - Contingency Planning	CP-7(2)	Alternate Processing Site | Accessibility	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.			x	x	
CP - Contingency Planning	CP-7(3)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).			x	x	
CP - Contingency Planning	CP-7(4)	Alternate Processing Site | Preparation for Use	Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-7(6)	Alternate Processing Site | Inability to Return to Primary Site	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-8	Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [information system operations] for essential mission and business functions within [the specified timeframes and metrics defined in the information system contingency plan (ISCP) and Business Impact Analysis (BIA)] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.			x	x	
CP - Contingency Planning	CP-8(1)	Telecommunications Services | Priority of Service Provisions	(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and (b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.			x	x	
CP - Contingency Planning	CP-8(2)	Telecommunications Services | Single Points of Failure	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.			x	x	
CP - Contingency Planning	CP-8(3)	Telecommunications Services | Separation of Primary and Alternate Providers	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.				x	
CP - Contingency Planning	CP-8(4)	Telecommunications Services | Provider Contingency Plan	(a) Require primary and alternate telecommunications service providers to have contingency plans; (b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and (c) Obtain evidence of contingency testing and training by providers [as needed but no less than annually].				x	
CP - Contingency Planning	CP-8(5)	Telecommunications Services | Alternate Telecommunication Service Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-9	System Backup	a. Conduct backups of user-level information contained in [the information system] [incremental daily backups and monthly full backups]; b. Conduct backups of system-level information contained in the system [incremental daily backups and monthly full backups]; c. Conduct backups of system documentation, including security- and privacy-related documentation [incremental daily backups and monthly full backups]; and d. Protect the confidentiality, integrity, and availability of backup information.		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-9(1)	System Backup | Testing for Reliability and Integrity	Test backup information [at least annually (i.e., each fiscal year)] to verify media reliability and information integrity.			x	x	
CP - Contingency Planning	CP-9(2)	System Backup | Test Restoration Using Sampling	Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.				x	
CP - Contingency Planning	CP-9(3)	System Backup | Separate Storage for Critical Information	Store backup copies of [current response plans and all supporting documentation, critical system software (including operating systems, cryptographic key management systems, and intrusion detection/prevention systems), as well as copies of the system inventory (including hardware, software, and firmware components)] in a separate facility or in a fire rated container that is not collocated with the operational system.				x	
CP - Contingency Planning	CP-9(5)	System Backup | Transfer to Alternate Storage Site	Transfer system backup information to the alternate storage site [at a transfer rate consistent with the specified timeframes and metrics defined in the information system contingency plan (ISCP) and Business Impact Analysis (BIA).]				x	
CP - Contingency Planning	CP-9(6)	System Backup | Redundant Secondary System	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-9(7)	System Backup | Dual Authorization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-9(8)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [all system backup information in storage at both primary and alternate locations, when an alternate location is required and in place].			x	x	
CP - Contingency Planning	CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [system-level specified recovery times and metrics defined in the information system contingency plan (ISCP) and Business Impact Analysis (BIA)] after a disruption, compromise, or failure.		x	x	x	
CP - Contingency Planning	CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	Implement transaction recovery for systems that are transaction-based.			x	x	
CP - Contingency Planning	CP-10(4)	System Recovery and Reconstitution | Restore Within Time Period	Provide the capability to restore system components within [system-level specified recovery times and metrics defined in the information system contingency plan (ISCP) and business impact analysis (BIA)] from configuration-controlled and integrity-protected information representing a known, operational state for the components.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
CP - Contingency Planning	CP-10(6)	System Recovery and Reconstitution | Component Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-11	Alternate Communications Protocols	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-12	Safe Mode	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
CP - Contingency Planning	CP-13	Alternative Security Mechanisms	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-1	Policy and Procedures	a. Develop, document, and disseminate to [all ED employees, contractors, and users that are authorized with 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)]: 1. [Department-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Department Chief Information Security Officer (CISO)] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current identification and authentication: 1. Policy [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]; and 2. 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].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IA - Identification and Authentication	IA-2	Identification and Authentication (organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.		x	x	x	
IA - Identification and Authentication	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.		x	x	x	
IA - Identification and Authentication	IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.		x	x	x	
IA - Identification and Authentication	IA-2(5)	Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.				x	
IA - Identification and Authentication	IA-2(6)	Identification and Authentication (organizational Users) | Access to Accounts — Separate Device	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts —	Implement replay-resistant authentication mechanisms for access to [privileged accounts and non-privileged accounts].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Replay Resistant						
IA - Identification and Authentication	IA-2(10)	Identification and Authentication (organizational Users) | Single Sign-on	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-2(12)	Identification and Authentication (organizational Users) | Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.		x	x	x	
IA - Identification and Authentication	IA-2(13)	Identification and Authentication (organizational Users) | Out-of-band Authentication	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-3	Device Identification and Authentication	Uniquely identify and authenticate [ED S/SO or Contractor recommended and ED-approved specific and/or types of devices] before establishing a [local, remote, or network] connection.			x	x	
IA - Identification and Authentication	IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-3(3)	Device Identification and Authentication | Dynamic Address Allocation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IA - Identification and Authentication	IA-3(4)	Device Identification and Authentication | Device Attestation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-4	Identifier Management	Manage system identifiers by: a. Receiving authorization from [Information System Owners or authorized delegate] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual, group, role, service, or device; and d. Preventing reuse of identifiers for [one year].		x	x	x	
IA - Identification and Authentication	IA-4(1)	Identifier Management | Prohibit Account Identifiers as Public Identifiers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-4(4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [federal employee, including unpaid positions, or contractor].			x	x	
IA - Identification and Authentication	IA-4(5)	Identifier Management | Dynamic Management	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-4(6)	Identifier Management | Cross-organization Management	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-4(8)	Identifier Management | Pairwise Pseudonymous Identifiers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-4(9)	Identifier Management | Attribute Maintenance and Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IA - Identification and Authentication	IA-5	Authenticator Management	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators [in accordance with Federal Zero Trust Strategy, Department Zero Trust Architecture Strategy/Plan or 90 days when zero trust architecture is not implemented] or when [compromised, recovered/forgotten, or due to incident related events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.		x	x	x	
IA - Identification and Authentication	IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication: (a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [annually (i.e., each fiscal year] and when organizational passwords are suspected to have been compromised directly or indirectly; (b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a); (c) Transmit passwords only over cryptographically-protected channels; (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash; (e) Require immediate selection of a new password upon account recovery; (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; (g) Employ automated tools to assist the user in selecting strong password authenticators; and (h) Enforce the following composition and complexity rules [Passwords must contain each of the following four types of characters: • English uppercase letters(A-Z) • English lowercase letters(a-z) • Arabic numerals (0-9) • Non-alphanumeric special characters ($,!, &, etc.) Password complexity is not required after implementation of zero trust architectures in accordance with Federal Zero Trust Strategy and/or Department Zero Trust Architecture Strategy/Plan.]		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IA - Identification and Authentication	IA-5(2)	Authenticator Management | Public Key-based Authentication	(a) For public key-based authentication: (1) Enforce authorized access to the corresponding private key; and (2) Map the authenticated identity to the account of the individual or group; and (b) When public key infrastructure (PKI) is used: (1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and (2) Implement a local cache of revocation data to support path discovery and validation.			x	x	
IA - Identification and Authentication	IA-5(5)	Authenticator Management | Change Authenticators Prior to Delivery	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(6)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.			x	x	
IA - Identification and Authentication	IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.					
IA - Identification and Authentication	IA-5(8)	Authenticator Management | Multiple System Accounts	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(9)	Authenticator Management | Federated Credential Management	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(10)	Authenticator Management | Dynamic Credential Binding	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(12)	Authenticator Management | Biometric Authentication Performance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IA - Identification and Authentication	IA-5(13)	Authenticator Management | Expiration of Cached Authenticators	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(14)	Authenticator Management | Managing Content of PKI Trust Stores	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(15)	Authenticator Management | GSA-approved Products and Services	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(16)	Authenticator Management | In-person or Trusted External Party Authenticator Issuance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(17)	Authenticator Management | Presentation Attack Detection for Biometric Authenticators	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-5(18)	Authenticator Management | Password Managers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identification and Authentication	IA-6	Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.		x	x	x	
IA - Identification and Authentication	IA-7	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.		x	x	x	
IA - Identification and	IA-8	Identification and Authentication	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Authentic ation		(non-organizational Users)						
IA - Identificat ion and Authentic ation	IA-8(1)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.		x	x	x	
IA - Identificat ion and Authentic ation	IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators	(a) Accept only external authenticators that are NIST-compliant; and (b) Document and maintain a list of accepted external authenticators.		x	x	x	
IA - Identificat ion and Authentic ation	IA-8(4)	Identification and Authentication (non-organizational Users) | Use of Defined Profiles	Conform to the approved profiles for identity management.		x	x	x	
IA - Identificat ion and Authentic ation	IA-8(5)	Identification and Authentication (non-organizational Users) | Acceptance of PIV-I Credentials	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identificat ion and Authentic ation	IA-8(6)	Identification and Authentication (non-organizational Users) | Disassociability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identificat	IA-9	Service Identification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
ion and Authentic ation		and Authentication						
IA - Identificat ion and Authentic ation	IA-10	Adaptive Authentication	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identificat ion and Authentic ation	IA-11	Re-authentication	Require users to re-authenticate when [required by zero trust architecture policies, standards, guidance and memorandums provided by CISA, OMB and NIST; re-establishing authenticated access following activation of a device lock (e.g., screensaver), passwords are reset, privileged functions are executed, and/or periodic reauthentication time limits are met.]		x	x	x	
IA - Identificat ion and Authentic ation	IA-12	Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence.			x	x	
IA - Identificat ion and Authentic ation	IA-12(1)	Identity Proofing | Supervisor Authorization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IA - Identificat ion and Authentic ation	IA-12(2)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.			x	x	
IA - Identificat ion and Authentic ation	IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification	Require that the presented identity evidence be validated and verified through [methods which are consistent with the risks to the systems, roles, and privileges associated with the users account].			x	x	
IA - Identificat ion and Authentic ation	IA-12(4)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IA - Identification and Authentication	IA-12(5)	Identity Proofing | Address Confirmation	Require that a [registration code or notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.			x	x	
IA - Identification and Authentication	IA-12(6)	Identity Proofing | Accept Externally-proofed Identities	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IR - Incident Response	IR-1	Policy and Procedures	a. 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)]: 1. [Department-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update the current incident response: 1. Policy [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]; and 2. 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].	x	x	x	x	
IR - Incident Response	IR-2	Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [thirty (30) days] of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. [at least annually (i.e., each fiscal year)] thereafter; and b. Review and update incident response training content [at least annually (i.e., each fiscal year)] and following [events tat may precipitate an update to incident response training content including, but not limited to , incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines].	x	x	x	x	
IR - Incident Response	IR-2(1)	Incident Response Training | Simulated Events	Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IR - Incident Response	IR-2(2)	Incident Response Training | Automated Training Environments	Provide an incident response training environment using [ED approved interactive simulations based on real-world data].				x	
IR - Incident Response	IR-2(3)	Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	x				
IR - Incident Response	IR-3	Incident Response Testing	Test the effectiveness of the incident response capability for the system [at least annually (i.e., each fiscal year)] using the following tests: [one or more of the following: tabletop or functional tests/checklist, strategic and tactical threat modeling, simulations, ad hoc penetration assessments, and other assessment methods identified and authorized by the Department].	x		x	x	
IR - Incident Response	IR-3(1)	Incident Response Testing | Automated Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-3(2)	Incident Response Testing | Coordination with Related Plans	Coordinate incident response testing with organizational elements responsible for related plans.			x	x	
IR - Incident Response	IR-3(3)	Incident Response Testing | Continuous Improvement	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4	Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	x	x	x	x	
IR - Incident Response	IR-4(1)	Incident Handling | Automated Incident Handling Processes	Support the incident handling process using [EDSOC automated mechanisms].			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IR - Incident Response	IR-4(2)	Incident Handling | Dynamic Reconfiguration	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(3)	Incident Handling | Continuity of Operations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(4)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.				x	
IR - Incident Response	IR-4(5)	Incident Handling | Automatic Disabling of System	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(6)	Incident Handling | Insider Threats	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(7)	Incident Handling | Insider Threats — Intra-organization Coordination	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(8)	Incident Handling | Correlation with External Organizations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(9)	Incident Handling | Dynamic Response Capability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(10)	Incident Handling | Supply Chain Coordination	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(11)	Incident Handling | Integrated Incident Response Team	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [30 days or less based upon availability of staffing, funding and tools].				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IR - Incident Response	IR-4(12)	Incident Handling | Malicious Code and Forensic Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(13)	Incident Handling | Behavior Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(14)	Incident Handling | Security Operations Center	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-4(15)	Incident Handling | Public Relations and Reputation Repair	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-5	Incident Monitoring	Track and document incidents.	x	x	x	x	
IR - Incident Response	IR-5(1)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis	Track incidents and collect and analyze incident information using [methodology within the Incident Response Plan (IRP)].				x	
IR - Incident Response	IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [immediately and without unreasonable delay]; and b. Report incident information to [the EDSOC and Information System Security Officer (ISSO)]	x	x	x	x	
IR - Incident Response	IR-6(1)	Incident Reporting | Automated Reporting	Report incidents using [methodology within the Incident Response Plan (IRP)].			x	x	
IR - Incident Response	IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-6(3)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IR - Incident Response	IR-7	Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	x	x	x	x	
IR - Incident Response	IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and Support	Increase the availability of incident response information and support using [ED approved automated mechanisms].			x	x	
IR - Incident Response	IR-7(2)	Incident Response Assistance | Coordination with External Providers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-8	Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [personnel responsible for SSP approval in accordance with the Department's required authorization documentation standards; the Authorizing Official (AO) or AO delegate (only if it is the first time the SSP is generated (initiation) OR if there a major change), the Information System Owner (ISO) and Information System Security Officer (ISSO) as part of the SSP review and approval processes] [at least annually]; and 10. Explicitly designates responsibility for incident response to [EDSOC]. b. Distribute copies of the incident response plan to [Information System Owner (ISO), Information System Security Officer (ISSO), and system personnel with incident response responsibilities]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Information System Owner (ISO), Information System Security Officer (ISSO) and system personnel with incident response responsibilities]; and e. Protect the incident response plan from unauthorized disclosure and modification.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
IR - Incident Response	IR-8(1)	Incident Response Plan | Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information: (a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; (b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and (c) Identification of applicable privacy requirements.	x				
IR - Incident Response	IR-9	Information Spillage Response	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-9(2)	Information Spillage Response | Training	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-9(3)	Information Spillage Response | Post-spill Operations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
IR - Incident Response	IR-9(4)	Information Spillage Response | Exposure to Unauthorized Personnel	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MA - Maintenance	MA-1	Policy and Procedures	a. 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)]: 1. [Department-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; b. Designate an [Department Chief Information Security Officer (CISO)] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and c. Review and update the current maintenance: 1. Policy [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]; and 2. 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].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MA - Maintenance	MA-2	Controlled Maintenance	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; c. Require that [the Information System Owner (ISO), Information System Security Officer (ISSO), or designated alternate] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [information the Department deems as sensitive, including but not limited to Personally Identifiable Information (PII), Sensitive PII, and Controlled Unclassified Information]; e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and f. Include the following information in organizational maintenance records: [(i)the date and time of maintenance, (ii) a description of the maintenance performed, (iii) names of the individuals or group performing the maintenance, (iv) name of the escort, and (v) system components or equipment that are removed or replaced].		x	x	x	
MA - Maintenance	MA-2(2)	Controlled Maintenance | Automated Maintenance Activities	(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [ED approved automated mechanisms]; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.				x	
MA - Maintenance	MA-3	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools [at least annually (i.e., each fiscal year)].			x	x	
MA - Maintenance	MA-3(1)	Maintenance Tools | Inspect Tools	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.			x	x	
MA - Maintenance	MA-3(2)	Maintenance Tools | Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are used in the system.			x	x	
MA - Maintenance	MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	Prevent the removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [the Information System Owner (ISO), Information System Security Officer (ISSO), or designated alternate] explicitly authorizing removal of the equipment from the facility.			x	x	
MA - Maintenance	MA-3(4)	Maintenance Tools | Restricted Tool Use	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MA - Maintenance	MA-3(5)	Maintenance Tools | Execution with Privilege	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-3(6)	Maintenance Tools | Software Updates and Patches	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-4	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintain records for nonlocal maintenance and diagnostic activities; and e. Terminate session and network connections when nonlocal maintenance is completed.		x	x	x	
MA - Maintenance	MA-4(1)	Nonlocal Maintenance | Logging and Review	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-4(3)	Nonlocal Maintenance | Comparable Security and Sanitization	(a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.				x	
MA - Maintenance	MA-4(4)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-4(5)	Nonlocal Maintenance | Approvals and Notifications	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-4(6)	Nonlocal Maintenance | Cryptographic Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-4(7)	Nonlocal Maintenance | Disconnect Verification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MA - Maintenance	MA-5	Maintenance Personnel	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.		x	x	x	
MA - Maintenance	MA-5(1)	Maintenance Personnel | Individuals Without Appropriate Access	(a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and (2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and (b) Develop and implement [alternate security safeguards and/or AO approved alternate controls defined in the security plan] in the event a system component cannot be sanitized, removed, or disconnected from the system.				x	
MA - Maintenance	MA-5(2)	Maintenance Personnel | Security Clearances for Classified Systems	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-5(3)	Maintenance Personnel | Citizenship Requirements for Classified Systems	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-5(4)	Maintenance Personnel | Foreign Nationals	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-5(5)	Maintenance Personnel | Non-system Maintenance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MA - Maintenance	MA-6	Timely Maintenance	Obtain maintenance support and/or spare parts for [security critical information system components and/or essential information technology components] within [system-level specified timeframes and metrics defined in the information system contingency plan (ISCP) and Business Impact Analysis (BIA)] of failure.			x	x	
MA - Maintenance	MA-6(1)	Timely Maintenance | Preventive Maintenance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-6(2)	Timely Maintenance | Predictive Maintenance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-6(3)	Timely Maintenance | Automated Support for Predictive Maintenance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MA - Maintenance	MA-7	Field Maintenance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MP - Media Protection	MP-1	Policy and Procedures	a. 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)]: 1. [Department-level] media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the media protection policy and procedures; and c. Review and update the current media protection: 1. Policy [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]; and 2. 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].	x	x	x	x	
MP - Media Protection	MP-2	Media Access	Restrict access to [digital media to include but not limited to: diskettes; magnetic tapes; external/removable hard disk drives; flash drives' compact disks; and digital video disks and non-digital media to include but not limited to: paper documents and microfilm] to [ED approved personnel and roles].		x	x	x	
MP - Media Protection	MP-3	Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempt [ED defined system media or hardware components] from marking if the media remain within [ED-controlled areas in accordance with OCIO: 3-112/ACSD-OCIO-004 (Cybersecurity Policy) and OCIO 3-113/ACSD-OCIO-002 (Controlled Unclassified Information Program) for media storing and/or processing CUI].			x	x	
MP - Media Protection	MP-4	Media Storage	a. Physically control and securely store [digital media to include but not limited to: diskettes; magnetic tapes; external/removable hard disk drives; flash drives' compact disks; and digital video disks and non-digital media to include but not limited to: paper documents and microfilm] within [ED secure/ controlled facilities]; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MP - Media Protection	MP-4(2)	Media Storage | Automated Restricted Access	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-5	Media Transport	a. Protect and control [digital media to include but not limited to: diskettes; magnetic tapes; external/removable hard disk drives; flash drives' compact disks; and digital video disks and non-digital media to include but not limited to: paper documents and microfilm] during transport outside of controlled areas using [a FIPS 140-2 validated encryption module/mechanism for digital assets and locked containers for physical assets]; b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the transport of system media; and d. Restrict the activities associated with the transport of system media to authorized personnel.			x	x	
MP - Media Protection	MP-5(3)	Media Transport | Custodians	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-6	Media Sanitization	a. Sanitize [all digital and non-digital information system media] prior to disposal, release out of organizational control, or release for reuse using [the current version of NIST SP 800-88 sanitization techniques and procedures to include, but not limited to: clearing; purging; cryptographic erase; de-identification of personally identifiable information; and destruction]; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	x	x	x	x	
MP - Media Protection	MP-6(1)	Media Sanitization | Review, Approve, Track, Document, and Verify	Review, approve, track, document, and verify media sanitization and disposal actions.				x	
MP - Media Protection	MP-6(2)	Media Sanitization | Equipment Testing	Test sanitization equipment and procedures [at least annually (i.e., each fiscal year)] to ensure that the intended sanitization is being achieved.				x	
MP - Media Protection	MP-6(3)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [(i) devices are purchased from manufacturers or vendors prior to initial use; (ii) unable to maintain a positive chain of custody for the devices].				x	
MP - Media Protection	MP-6(7)	Media Sanitization | Dual Authorization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
MP - Media Protection	MP-6(8)	Media Sanitization | Remote Purging or Wiping of Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-7	Media Use	a. [Restrict] the use of [non-FIPS 140-2 compliant digital storage devices, to include but not limited to: backup media, removable media, and mobile devices] on [all ED information systems] using [ED approved technical and non-technical security safeguards]; and b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.		x	x	x	
MP - Media Protection	MP-7(2)	Media Use | Prohibit Use of Sanitization-resistant Media	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-8	Media Downgrading	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-8(1)	Media Downgrading | Documentation of Process	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-8(2)	Media Downgrading | Equipment Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-8(3)	Media Downgrading | Controlled Unclassified Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
MP - Media Protection	MP-8(4)	Media Downgrading | Classified Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-1	Policy and Procedures	a. 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)]: 1. [Department-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; b. Designate an [Deputy Assistant Secretary, Office of Security, Facilities, and Logistics within the Office of Finance and Operations (OFO)] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and c. Review and update the current physical and environmental protection: 1. Policy [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]; and 2. 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].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-2	Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [at least annually (i.e., each fiscal year)]; and d. Remove individuals from the facility access list when access is no longer required.		x	x	x	
PE - Physical and Environmental Protection	PE-2(1)	Physical Access Authorizations | Access by Position or Role	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-2(2)	Physical Access Authorizations | Two Forms of Identification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-2(3)	Physical Access Authorizations | Restrict Unescorted Access	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-3	Physical Access Control	a. Enforce physical access authorizations at [designated entry/exit facility access points and interior access points to the system and components] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [using physical access devices such as keys, locks, combinations, biometric readers, card readers, devices and/or guards based upon an assessment of risk]; b. Maintain physical access audit logs for [all facility entry/exit points]; c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [risk appropriate security safeguards]; d. Escort visitors and control visitor activity [individuals requiring visitor escorts and monitoring in non public areas]; e. Secure keys, combinations, and other physical access devices; f. Inventory [all physical access devices] every [fiscal year, at a minimum]; and g. Change combinations and keys [at least annually (i.e., each fiscal year)] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.		x	x	x	
PE - Physical and Environmental Protection	PE-3(1)	Physical Access Control | System Access	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [designated entry/exit facility access points and interior access points to the system and components].				x	
PE - Physical and	PE-3(2)	Physical Access Control |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Environmental Protection		Facility and Systems						
PE - Physical and Environmental Protection	PE-3(3)	Physical Access Control | Continuous Guards	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-3(4)	Physical Access Control | Lockable Casings	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-3(5)	Physical Access Control | Tamper Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-3(7)	Physical Access Control | Physical Barriers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-3(8)	Physical Access Control | Access Control Vestibules	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-4	Access Control for Transmission	Control physical access to [system distribution and transmission lines to include, network circuits from the areas within the facility designated for housing the system components] within organizational facilities using [physical security safeguards to include but not limited to: locked wiring closets; disconnected or locked spare jacks; and/or protection of cabling by conduit or cable trays]			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-5	Access Control for Output Devices	Control physical access to output from [devices (e.g., monitors, printers, scanners, audio devices, facsimile machines, copiers, etc.) connected to information systems processing sensitive information] to prevent unauthorized individuals from obtaining the output.			x	x	
PE - Physical and Environmental Protection	PE-5(2)	Access Control for Output Devices | Link to Individual Identity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-6	Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [as needed] and upon occurrence of [events or potential indications of events including, but not limited to, suspicious physical activities such as excessive access outside of normal work hours, repeated access to areas not normally accessed, out of sequence access]; and c. Coordinate results of reviews and investigations with the organizational incident response capability.		x	x	x	
PE - Physical and Environmental	PE-6(1)	Monitoring Physical Access | Intrusion Alarms and	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection		Surveillance Equipment						
PE - Physical and Environmental Protection	PE-6(2)	Monitoring Physical Access | Automated Intrusion Recognition and Responses	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-6(3)	Monitoring Physical Access | Video Surveillance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-6(4)	Monitoring Physical Access | Monitoring Physical Access to Systems	Monitor physical access to the system in addition to the physical access monitoring of the facility at [facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, and server rooms and media storage areas].				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-8	Visitor Access Records	a. Maintain visitor access records to the facility where the system resides for [at least three (3) years]; b. Review visitor access records [on an as needed basis]; and c. Report anomalies in visitor access records to [facility security staff, the Information System Owner (ISO) and Information System Security Officer (ISSO)].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-8(1)	Visitor Access Records | Automated Records Maintenance and Review	Maintain and review visitor access records using [available, ED approved automated mechanisms].				x	
PE - Physical and Environmental Protection	PE-8(3)	Visitor Access Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [visitor first and last name, organization, purpose of visit, dates/times of visit, as well as first and last name of facility escort].	x				
PE - Physical and Environmental Protection	PE-9	Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-9(1)	Power Equipment and Cabling | Redundant Cabling	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-9(2)	Power Equipment and Cabling | Automatic Voltage Controls	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-10	Emergency Shutoff	a. Provide the capability of shutting off power to [information systems or individual system components] in emergency situations; b. Place emergency shutoff switches or devices in [facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, and server rooms)] to facilitate access for authorized personnel; and c. Protect emergency power shutoff capability from unauthorized activation.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-11	Emergency Power	Provide an uninterruptible power supply to facilitate [an orderly shutdown of the information system and/or transition of the information system to long-term alternate power] in the event of a primary power source loss.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-11(1)	Emergency Power | Alternate Power Supply — Minimal Operational Capability	Provide an alternate power supply for the system that is activated [automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.				x	
PE - Physical and Environmental Protection	PE-11(2)	Emergency Power | Alternate Power Supply — Self-contained	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental	PE-12	Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection								
PE - Physical and Environmental Protection	PE-12(1)	Emergency Lighting | Essential Mission and Business Functions	Provide emergency lighting for all areas within the facility supporting essential mission and business functions.					
PE - Physical and Environmental Protection	PE-13	Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.		x	x	x	
PE - Physical and Environmental Protection	PE-13(1)	Fire Protection | Detection Systems – Automatic Activation and Notification	Employ fire detection systems that activate automatically and notify [facility personnel or roles with facility management and/or physical security responsibilities] and [emergency responders (e.g. Police and Fire Department)] in the event of a fire.			x	x	
PE - Physical and Environmental Protection	PE-13(2)	Fire Protection | Suppression Systems – Automatic Activation and Notification	(a) Employ fire suppression systems that activate automatically and notify [facility personnel or roles with facility management and/or physical security responsibilities] and [emergency responders (e.g. Police and Fire Department)]; and (b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.				x	
PE - Physical and Environmental Protection	PE-13(4)	Fire Protection | Inspections	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-14	Environmental Controls	a. Maintain [temperature and humidity] levels within the facility where the system resides at [acceptable levels which ensure systems and equipment operate within vendor recommended limits, if any, and ranges consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines for temperature and humidity]; and b. Monitor environmental control levels [continuously].		x	x	x	
PE - Physical and Environmental Protection	PE-14(1)	Environmental Controls | Automatic Controls	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-14(2)	Environmental Controls | Monitoring with Alarms and Notifications	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-15	Water Damage Protection	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.		x	x	x	
PE - Physical and Environmental Protection	PE-15(1)	Water Damage Protection | Automation Support	Detect the presence of water near the system and alert [ED designated personnel or roles with Physical Security Program responsibilities] using [ED approved automated mechanisms such as notification systems, water detection sensors and alarms].				x	
PE - Physical and Environmental	PE-16	Delivery and Removal	a. Authorize and control [all information system components] entering and exiting the facility; and b. Maintain records of the system components.		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection								
PE - Physical and Environmental Protection	PE-17	Alternate Work Site	a. Determine and document the [ED approved alternate work sites] allowed for use by employees; b. Employ the following controls at alternate work sites: [controls defined within ED directives, policies, including but not limited to OCIO: 3-112/ACSD-OCIO-004 (Cybersecurity Policy)]; c. Assess the effectiveness of controls at alternate work sites; and d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.			x	x	
PE - Physical and Environmental Protection	PE-18	Location of System Components	Position system components within the facility to minimize potential damage from [physical and environmental hazards] and to minimize the opportunity for unauthorized access.				x	
PE - Physical and Environmental Protection	PE-19	Information Leakage	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-19(1)	Information Leakage | National Emissions and Tempest Policies and Procedures	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-20	Asset Monitoring and Tracking	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-21	Electromagnetic Pulse Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PE - Physical and Environmental Protection	PE-22	Component Marking	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PE - Physical and Environmental Protection	PE-23	Facility Location	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PL - Planning	PL-1	Policy and Procedures	a. 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]: 1. [Department-level] planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the planning policy and procedures; and c. Review and update the current planning: 1. Policy [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]; and 2. 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].	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PL - Planning	PL-2	System Security and Privacy Plans	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of mission and business processes; 4. Identify the individuals that fulfill system roles and responsibilities; 5. Identify the information types processed, stored, and transmitted by the system; 6. Provide the security categorization of the system, including supporting rationale; 7. Describe any specific threats to the system that are of concern to the organization; 8. Provide the results of a privacy risk assessment for systems processing personally identifiable information; 9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components; 10. Provide an overview of the security and privacy requirements for the system; 11. Identify any relevant control baselines or overlays, if applicable; 12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; 13. Include risk determinations for security and privacy architecture and design decisions; 14. Include security- and privacy-related activities affecting the system that require planning and coordination with [other individuals or groups within the organization, including but limiting to, those responsible for assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing, as required]; and 15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation. b. Distribute copies of the plans and communicate subsequent changes to the plans to [personnel with cybersecurity and privacy responsibilities, including but not limited to the Authorizing Official (AO) or AO delegate, Information System Security Officer (ISSO), and Information System Owner (ISO)]; c. Review the plans [at least annually or when a major change occurs to the system]; d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and e. Protect the plans from unauthorized disclosure and modification.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PL - Planning	PL-4	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c. Review and update the rules of behavior [annually (i.e., each fiscal year)]; and d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [when the rules are revised or updated].	x	x	x	x	
PL - Planning	PL-4(1)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	Include in the rules of behavior, restrictions on: (a) Use of social media, social networking sites, and external sites/applications; (b) Posting organizational information on public websites; and (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.	x	x	x	x	
PL - Planning	PL-7	Concept of Operations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PL - Planning	PL-8	Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [at least annually, and update as necessary, in conjunction with SSP reviews/updates] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	x		x	x	
PL - Planning	PL-8(1)	Security and Privacy Architectures | Defense in Depth	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PL - Planning	PL-8(2)	Security and Privacy Architectures |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Supplier Diversity						
PL - Planning	PL-9	Central Management	Centrally manage [planning, implementing, assessing, authorizing, and monitoring the Department-defined, centrally managed controls and processes used to support common (inherited) controls within the Department's enterprise tool, Cyber Security Assessment & Management (CSAM)].	x				
PL - Planning	PL-10	Baseline Selection	Select a control baseline for the system.		x	x	x	
PL - Planning	PL-11	Baseline Tailoring	Tailor the selected control baseline by applying specified tailoring actions.		x	x	x	
PM - Program Management	PM-1	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Review and update the organization-wide information security program plan [annually (i.e., each fiscal year)] and following [organizational changes and identification of problems during plan implementation or security control assessments]; and c. Protect the information security program plan from unauthorized disclosure and modification.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-2	Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-3	Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PM - Program Management	PM-4	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with established reporting requirements. b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-5	System Inventory	Develop and update [quarterly] an inventory of organizational systems.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [quarterly] an inventory of all systems, applications, and projects that process personally identifiable information.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-6	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-7	Enterprise Architecture	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-7(1)	Enterprise Architecture | Offloading	Offload [ED approved supportive but non-essential functions, as feasible,] to other systems, system components, or an external provider.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-8	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PM - Program Management	PM-9	Risk Management Strategy	a. Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; b. Implement the risk management strategy consistently across the organization; and c. Review and update the risk management strategy [annually (i.e., each fiscal year)] or as required, to address organizational changes.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-10	Authorization Process	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Integrate the authorization processes into an organization-wide risk management program.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-11	Mission and Business Process Definition	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and c. Review and revise the mission and business processes [annually (i.e., each fiscal year)].	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-12	Insider Threat Program	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PM - Program Management	PM-14	Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-15	Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and c. To share current security and privacy information, including threats, vulnerabilities, and incidents.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-16	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-16(1)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PM - Program Management	PM-17	Protecting Controlled Unclassified Information on External Systems	a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and b. Review and update the policy and procedures [annually (i.e., each fiscal year)].	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-18	Privacy Program Plan	a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: 1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; 2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; 3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; 4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program; 5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and 6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and b. Update the plan [annually (i.e., each fiscal year)] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PM - Program Management	PM-19	Privacy Program Leadership Role	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-20	Dissemination of Privacy Program Information	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are publicly available; and c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-20(1)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that: (a) Are written in plain language and organized in a way that is easy to understand and navigate; (b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and (c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-21	Accounting of Disclosures	a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including: 1. Date, nature, and purpose of each disclosure; and 2. Name and address, or other contact information of the individual or organization to which the disclosure was made; b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d. Appeals of adverse decisions on correction or deletion requests.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-23	Data Governance Body	Establish a Data Governance Body consisting of [roles as defined in the ED Data Governance Board (DGB) Charter, lead by the Chief Data Officer (CDO)] with [responsibilities as defined in the ED DGB Charter].		N/A - Deployed organiza	N/A - Deployed organization-wide	N/A - Deployed organiza	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
					tion-wide		tion-wide	
PM - Program Management	PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d. Review and update policies and procedures [annually (i.e., each fiscal year)].	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints; c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [30 Days]; d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [7 days]; and e. Response to complaints, concerns, or questions from individuals within [45 days].	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-27	Privacy Reporting	a. Develop [privacy reports] and disseminate to: 1. [OMB, US Congress] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and 2. [Inspector General and other officials as required] and other personnel with responsibility for monitoring privacy program compliance; and b. Review and update privacy reports [annually].	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-28	Risk Framing	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; b. Distribute the results of risk framing activities to [CIO, CISO, CPO/SAOP, and mission/business owners]; and c. Review and update risk framing considerations [annually (i.e., each fiscal year)].	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PM - Program Management	PM-29	Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-30	Supply Chain Risk Management Strategy	a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; b. Implement the supply chain risk management strategy consistently across the organization; and c. Review and update the supply chain risk management strategy on [annually (i.e., each fiscal year)] or as required, to address organizational changes.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-30(1)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PM - Program Management	PM-31	Continuous Monitoring Strategy	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [metrics as defined in IAS ISCM Roadmap]; b. Establishing [at least monthly] for monitoring and [annually (i.e., each fiscal year)] for assessment of control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and f. Reporting the security and privacy status of organizational systems to [CISO, CPO/SAOP] [monthly].	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	
PM - Program Management	PM-32	Purposing	Analyze [all FISMA information systems and services] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PS - Personnel Security	PS-1	Policy and Procedures	a. 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)]: 1. [Department-level] personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls; b. Designate an [Personnel Security Director] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and c. Review and update the current personnel security: 1. Policy [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]; and 2. 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].		x	x	x	
PS - Personnel Security	PS-2	Position Risk Designation	a. Assign a risk designation to all organizational positions; b. Establish screening criteria for individuals filling those positions; and c. Review and update position risk designations [every five (5) years for federal employees; during contract solicitation for contractor position risk designations in accordance with OFO-O: 5-101/ACSD-OFO-013 (Contractor Employee Personnel Security Screenings)].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PS - Personnel Security	PS-3	Personnel Screening	a. Screen individuals prior to authorizing access to the system; and b. Rescreen individuals in accordance with [requirements specified in OFO - O: 5-102 Federal Employee Personnel Security Screening and OFO-O: 5-101 Contractor Employee Personnel Security Screenings].		x	x	x	
PS - Personnel Security	PS-3(1)	Personnel Screening | Classified Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PS - Personnel Security	PS-3(2)	Personnel Screening | Formal Indoctrination	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PS - Personnel Security	PS-3(3)	Personnel Screening | Information with Special Protective Measures	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PS - Personnel Security	PS-3(4)	Personnel Screening | Citizenship Requirements	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PS - Personnel Security	PS-4	Personnel Termination	Upon termination of individual employment: a. Disable system access within [as soon as possible but no later than one business day after notifying the Help Desk]; b. Terminate or revoke any authenticators and credentials associated with the individual; c. Conduct exit interviews that include a discussion of [topics to include but not limited to: security constraints, proper accountability, nondisclosure agreements, and limitations on future employment]; d. Retrieve all security-related organizational system-related property; and e. Retain access to organizational information and systems formerly controlled by terminated individual.		x	x	x	
PS - Personnel Security	PS-4(1)	Personnel Termination | Post-employment Requirements	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PS - Personnel Security	PS-4(2)	Personnel Termination | Automated Actions	Use [ED approved automated mechanisms] to [notify [personnel with separation responsibilities as defined in the ED OM: 3-104/ ACSD-OFO-011 (Clearance of Personnel for Separation or Transfer), to include but not limited to security personnel (i.e. ISSO, Helpdesk)] of individual termination actions; disable access to system resources]				x	
PS - Personnel Security	PS-5	Personnel Transfer	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiate [ED transfer or reassignment actions] within [five (5) business days following the formal transfer action]; c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notify [ED personnel and/or roles as defined in the OM: 3-104/ ACSD-OFO-011 (Clearance of Personnel for Separation or Transfer)] within [twenty-four (24) hours)].		x	x	x	
PS - Personnel Security	PS-6	Access Agreements	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements [at least annually (i.e., each fiscal year)]; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [at least annually (i.e., each fiscal year)].	x	x	x	x	
PS - Personnel Security	PS-6(2)	Access Agreements | Classified Information Requiring Special Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
PS - Personnel Security	PS-6(3)	Access Agreements | Post-employment Requirements	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PS - Personnel Security	PS-7	External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization; c. Document personnel security requirements; d. Require external providers to notify [Contracting Officer Representative (COR), key personnel and personnel with privileged access] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [twenty-four (24) hours to forty-eight (48) hours]; and e. Monitor provider compliance with personnel security requirements.		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PS - Personnel Security	PS-8	Personnel Sanctions	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and b. Notify [all appropriate personnel and offices, to include but not limited to Personnel Security, OFO/OHR, OCIO, COR and/or supervisors or employee representatives, as appropriate] within [twenty-four (24) hours to forty eight (48) hours] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.		x	x	x	
PS - Personnel Security	PS-9	Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PT - Personally Identifiable Information Processing and Transparency	PT-1	Policy and Procedures	a. 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)]: 1. [Department-level] personally identifiable information processing and transparency policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls; b. Designate an [Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and c. Review and update the current personally identifiable information processing and transparency: 1. Policy [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]; and 2. 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].	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-2	Authority to Process Personally Identifiable Information	a. Determine and document the [authority as defined in the PIA] that permits the [processing as defined in the PIA] of personally identifiable information; and b. Restrict the [processing as defined in the PIA] of personally identifiable information to only that which is authorized.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processin	PT-2(1)	Authority to Process Personally Identifiable Information | Data Tagging	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
g and Transparency								
PT - Personally Identifiable Information Processing and Transparency	PT-2(2)	Authority to Process Personally Identifiable Information | Automation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-3	Personally Identifiable Information Processing Purposes	a. Identify and document the [purposes as defined in the PIA] for processing personally identifiable information; b. Describe the purpose(s) in the public privacy notices and policies of the organization; c. Restrict the [processing of data as defined in the PIA] of personally identifiable information to only that which is compatible with the identified purpose(s); and d. Monitor changes in processing personally identifiable information and implement [mechanisms as defined in the PIA] to ensure that any changes are made in accordance with [existing ED privacy policies].	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-3(1)	Personally Identifiable Information Processing Purposes | Data Tagging	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-3(2)	Personally Identifiable Information Processing Purposes | Automation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PT - Personally Identifiable Information Processing and Transparency	PT-4	Consent	Implement [mechanisms as defined in the PIA] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-4(1)	Consent | Tailored Consent	Provide [mechanisms as defined in the PIA] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-4(2)	Consent | Just-in-time Consent	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-4(3)	Consent | Revocation	Implement [mechanisms as defined in the PIA] for individuals to revoke consent to the processing of their personally identifiable information.		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PT - Personally Identifiable Information Processing and Transparency	PT-5	Privacy Notice	Provide notice to individuals about the processing of personally identifiable information that: a. Is available to individuals upon first interacting with an organization, and subsequently at [when changes to the processing of PII requires notification]; b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language; c. Identifies the authority that authorizes the processing of personally identifiable information; d. Identifies the purposes for which personally identifiable information is to be processed; and e. Includes [other information as stated in the PIA].	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-5(1)	Privacy Notice | Just-in-time Notice	Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-5(2)	Privacy Notice | Privacy Act Statements	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-6	System of Records Notice	For systems that process information that will be maintained in a Privacy Act system of records: a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review; b. Publish system of records notices in the Federal Register; and c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Informati	PT-6(1)	System of Records Notice | Routine Uses	Review all routine uses published in the system of records notice [Biennially] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.	x	Not allocated to security control	Not allocated to security	Not allocated to security control	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
on Processing and Transparency					baselines	control baselines	baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-6(2)	System of Records Notice | Exemption Rules	Review all Privacy Act exemptions claimed for the system of records at [Biennially] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-7	Specific Categories of Personally Identifiable Information	Apply [any processing conditions as defined in the PIA] for specific categories of personally identifiable information.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-7(1)	Specific Categories of Personally Identifiable Information | Social Security Numbers	When a system processes Social Security numbers: (a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier; (b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and (c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
PT - Personally Identifiable Information Processing and Transparency	PT-7(2)	Specific Categories of Personally Identifiable Information | First Amendment Information	Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
PT - Personally Identifiable Information Processing and Transparency	PT-8	Computer Matching Requirements	When a system or organization processes information for the purpose of conducting a matching program: a. Obtain approval from the Data Integrity Board to conduct the matching program; b. Develop and enter into a computer matching agreement; c. Publish a matching notice in the Federal Register; d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	
RA - Risk Assessment	RA-1	Policy and Procedures	a. 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)]: 1. [Department-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: 1. Policy [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]; and 2. 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].	x	x	x	x	
RA - Risk Assessment	RA-2	Security Categorization	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.		x	x	x	
RA - Risk Assessment	RA-2(1)	Security Categorization | Impact-level Prioritization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
RA - Risk Assessment	RA-3	Risk Assessment	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [the Security Assessment Report (SAR); the Privacy Impact Assessment (PIA), when a PIA is required; and the Facility Risk Assessment Report, required when a general support system or other hosting facility is deployed in a traditional datacenter]; d. Review risk assessment results [annually or whenever an update to the risk assessment is made]; e. Disseminate risk assessment results to [Authorizing Official (AO), Chief Information Security Officer (CISO), Chief Privacy Officer (CPO)/Senior Agency Official for Privacy (SAOP), Information System Owner (ISO), Information System Security Officer (ISSO)]; and f. Update the risk assessment [in accordance with the frequency defined in Department policy for each risk result documentation type] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
RA - Risk Assessment	RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	(a) Assess supply chain risks associated with [ED systems, components, and services as defined in the ICT SCRM Roadmap and Plan]; and (b) Update the supply chain risk assessment [annually or as defined in the ED ICT SCRM Roadmap and Plan], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.		x	x	x	
RA - Risk Assessment	RA-3(2)	Risk Assessment | Use of All-source Intelligence	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
RA - Risk Assessment	RA-3(3)	Risk Assessment | Dynamic Threat Awareness	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
RA - Risk Assessment	RA-3(4)	Risk Assessment | Predictive Cyber Analytics	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
RA - Risk Assessment	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [authenticated Operating System (OS) scans are conducted at a minimum on a weekly basis, authenticated Web Application and Database Application scans are conducted at a minimum on a monthly basis (or as needed to be more frequent), public facing systems enrolled in the National Cybersecurity Assessments and Technical Services (NCATS) "Cyber Hygiene" program are scanned at a NCATS defined frequency] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [(1) for externally facing systems (including High Value Assets (HVAs) and systems or assets with FIPS 199 High categorization) as follows: (a) Zero-Day scan vulnerabilities must be remediated within 24-48 hours of initial detection; (b) Any Critical (Very High) scan vulnerabilities must be remediated within 15 calendar days of initial detection;. (c) Any High scan vulnerabilities must be remediated within 30 calendar days of initial detection. (d) Any Moderate scan vulnerabilities must be remediated within 90 calendar days of initial detection; (d) Any Low scan vulnerabilities must be remediated within 180 calendar days of initial detection; (2) For internally facing systems only, system stakeholders are allowed 30 days analysis before the above set timeline commences.] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Information System owners (ISO), Information System Security Officers (ISSOs), and other relevant system stakeholders] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.		x	x	x	
RA - Risk Assessment	RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [no more than 24 hours prior to conducting a scan and in accordance with each tool's vendor data definition releases].		x	x	x	
RA - Risk Assessment	RA-5(3)	Vulnerability Monitoring and Scanning |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Breadth and Depth of Coverage						
RA - Risk Assessment	RA-5(4)	Vulnerability Monitoring and Scanning | Discoverable Information	Determine information about the system that is discoverable and take [the following actions: a. Notify ED-defined security personnel to include the Information System Security Officer (ISSO), move or obfuscate the discoverable information or take other actions, as appropriate; and b. Share the discoverable information with the EDSOC within one (1) hour of identification if it is determined that knowledge of the discoverable information could be detrimental to a system's security]				x	
RA - Risk Assessment	RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	Implement privileged access authorization to [all information system components as applicable (e.g., OS, DB, Web App, etc.] for [all vulnerability scanning activities].			x	x	
RA - Risk Assessment	RA-5(6)	Vulnerability Monitoring and Scanning | Automated Trend Analyses	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
RA - Risk Assessment	RA-5(8)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
RA - Risk Assessment	RA-5(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
RA - Risk Assessment	RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.		x	x	x	
RA - Risk Assessment	RA-6	Technical Surveillance Countermeasures Survey	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
RA - Risk Assessment	RA-7	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
RA - Risk Assessment	RA-8	Privacy Impact Assessments	Conduct privacy impact assessments for systems, programs, or other activities before: a. Developing or procuring information technology that processes personally identifiable information; and b. Initiating a new collection of personally identifiable information that: 1. Will be processed using information technology; and 2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.	x				
RA - Risk Assessment	RA-9	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [All FISMA reportable systems and critical system components] at [initially at the system design/architectural design phase of the Enterprise Program Management Review Framework (EPMR) and continuously through the entire lifecycle, including O&M phase if there are significant system changes impacting criticality of system components].			x	x	
RA - Risk Assessment	RA-10	Threat Hunting	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-1	Policy and Procedures	a. 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), OCIO: 3-110/ACSD-OCIO-011 (Software Asset Management Acquisition Policy), OFO-F: 2-107/ACSD-OFO-006 (Acquisition Planning), Acquisition Procedures Manual, and Security and Privacy Requirements for IT Procurements]: 1. [Department-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP) and Senior Procurement Executive or designee] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c. Review and update the current system and services acquisition: 1. Policy [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]; and 2. 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].	x	x	x	x	
SA - System and Services Acquisition	SA-2	Allocation of Resources	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-3	System Development Life Cycle	a. Acquire, develop, and manage the system using [OCIO: 1-016 Lifecycle Management (LCM) Framework and associated EPMR Framework] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	x	x	x	x	
SA - System and Services Acquisition	SA-3(1)	System Development Life Cycle | Manage Preproduction Environment	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-3(2)	System Development Life Cycle | Use of Live or Operational Data	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-3(3)	System Development Life Cycle | Technology Refresh	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-4	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Security and Privacy Requirements for IT Procurements] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-4(1)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.			x	x	
SA - System and Services Acquisition	SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [security-relevant external system interfaces; high-level design; low-level design; source code (only if applicable) or hardware schematics; and information and information sensitivity at level of detail necessary to permit analysis and testing].			x	x	
SA - System and Services Acquisition	SA-4(3)	Acquisition Process | Development Methods, Techniques, and Practices	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-4(5)	Acquisition Process | System, Component, and Service Configurations	Require the developer of the system, system component, or system service to: (a) Deliver the system, component, or service with [ED approved security configurations consistent with the Department's baseline security and privacy configuration settings documented in CM-6] implemented; and (b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.				x	
SA - System and Services Acquisition	SA-4(6)	Acquisition Process | Use of Information Assurance Products	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-4(7)	Acquisition Process | NIAP-approved Protection Profiles	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-4(8)	Acquisition Process | Continuous Monitoring Plan for Controls	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services	SA-4(9)	Acquisition Process | Functions, Ports,	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Acquisition		Protocols, and Services in Use						
SA - System and Services Acquisition	SA-4(10)	Acquisition Process | Use of Approved PIV Products	Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.		x	x	x	
SA - System and Services Acquisition	SA-4(11)	Acquisition Process | System of Records	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-4(12)	Acquisition Process | Data Ownership	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-5	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; b. Obtain or develop user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [action to create documentation if such documentation is essential to the effective implementation or operation of security controls] in response; and d. Distribute documentation to [Information System Owner (ISO) and Information System Security Officer (ISSO); in addition, distribute to other personnel with a need to know when required by contract or to provide system support].		x	x	x	
SA - System and Services Acquisition	SA-8	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [ED defined systems security and privacy engineering principles as documented in the ED Technical Security Architecture].		x	x	x	
SA - System and Services Acquisition	SA-8(1)	Security and Privacy Engineering Principles | Clear Abstractions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(2)	Security and Privacy Engineering Principles | Least Common Mechanism	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-8(3)	Security and Privacy Engineering Principles | Modularity and Layering	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(4)	Security and Privacy Engineering Principles | Partially Ordered Dependencies	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(5)	Security and Privacy Engineering Principles | Efficiently Mediated Access	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(6)	Security and Privacy Engineering Principles | Minimized Sharing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(7)	Security and Privacy Engineering Principles | Reduced Complexity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(8)	Security and Privacy Engineering Principles | Secure Evolvability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(9)	Security and Privacy Engineering Principles | Trusted Components	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and	SA-8(10)	Security and Privacy Engineering	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Services Acquisition		Principles | Hierarchical Trust						
SA - System and Services Acquisition	SA-8(11)	Security and Privacy Engineering Principles | Inverse Modification Threshold	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(12)	Security and Privacy Engineering Principles | Hierarchical Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(13)	Security and Privacy Engineering Principles | Minimized Security Elements	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(14)	Security and Privacy Engineering Principles | Least Privilege	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(15)	Security and Privacy Engineering Principles | Predicate Permission	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(16)	Security and Privacy Engineering Principles | Self-reliant Trustworthiness	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services	SA-8(17)	Security and Privacy Engineering Principles | Secure	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Acquisition		Distributed Composition						
SA - System and Services Acquisition	SA-8(18)	Security and Privacy Engineering Principles | Trusted Communications Channels	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(19)	Security and Privacy Engineering Principles | Continuous Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(20)	Security and Privacy Engineering Principles | Secure Metadata Management	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(21)	Security and Privacy Engineering Principles | Self-analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(22)	Security and Privacy Engineering Principles | Accountability and Traceability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(23)	Security and Privacy Engineering Principles | Secure Defaults	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services	SA-8(24)	Security and Privacy Engineering Principles |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Acquisition		Secure Failure and Recovery						
SA - System and Services Acquisition	SA-8(25)	Security and Privacy Engineering Principles | Economic Security	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(26)	Security and Privacy Engineering Principles | Performance Security	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(27)	Security and Privacy Engineering Principles | Human Factored Security	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(28)	Security and Privacy Engineering Principles | Acceptable Security	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(29)	Security and Privacy Engineering Principles | Repeatable and Documented Procedures	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(30)	Security and Privacy Engineering Principles | Procedural Rigor	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services	SA-8(31)	Security and Privacy Engineering Principles |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Acquisition		Secure System Modification						
SA - System and Services Acquisition	SA-8(32)	Security and Privacy Engineering Principles | Sufficient Documentation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-8(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [processes consistent with applicable laws and policies which ensure systems only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and only maintain personally identifiable information for as long as is necessary to accomplish the purpose].	x				

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-9	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [the ED-defined baseline security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [as specified in Security and Privacy Requirements for IT Procurements document and applicable external system services documentation to include service level agreements (SLAs].	x	x	x	x	
SA - System and Services Acquisition	SA-9(1)	External System Services | Risk Assessments and Organizational Approvals	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [all ED information systems and services which require an ATO].			x	x	
SA - System and Services Acquisition	SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-9(4)	External System Services | Consistent Interests of Consumers and Providers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-9(5)	External System Services | Processing, Storage, and Service Location	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-9(6)	External System Services | Organization-controlled Cryptographic Keys	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-9(7)	External System Services | Organization-controlled Integrity Checking	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-9(8)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-10	Developer Configuration Management	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [design, development, implementation, operations, and disposal]; b. Document, manage, and control the integrity of changes to [(ED defined configuration management items to include but not limited to : the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation.] c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [the Information System Owner (ISO) and Information System Security Officer (ISSO)]			x	x	
SA - System and Services Acquisition	SA-10(1)	Developer Configuration Management | Software and Firmware Integrity Verification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-10(2)	Developer Configuration Management | Alternative Configuration Management	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-10(3)	Developer Configuration Management | Hardware Integrity Verification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services	SA-10(4)	Developer Configuration Management | Trusted Generation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Acquisition								
SA - System and Services Acquisition	SA-10(5)	Developer Configuration Management | Mapping Integrity for Version Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-10(6)	Developer Configuration Management | Trusted Distribution	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-10(7)	Developer Configuration Management | Security and Privacy Representatives	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-11	Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [unit; integration; system; and/or regression] testing/evaluation [as defined in the configuration management plan] at [a depth and coverage necessary to ensure that required security controls are implemented correctly and operating as intended]; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.	x		x	x	
SA - System and Services Acquisition	SA-11(1)	Developer Testing and Evaluation | Static Code Analysis	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.					
SA - System and Services	SA-11(2)	Developer Testing and Evaluation | Threat	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Acquisition		Modeling and Vulnerability Analyses						
SA - System and Services Acquisition	SA-11(3)	Developer Testing and Evaluation | Independent Verification of Assessment Plans and Evidence	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-11(4)	Developer Testing and Evaluation | Manual Code Reviews	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-11(5)	Developer Testing and Evaluation | Penetration Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-11(6)	Developer Testing and Evaluation | Attack Surface Reviews	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-11(7)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-11(8)	Developer Testing and Evaluation | Dynamic Code Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services	SA-11(9)	Developer Testing and Evaluation | Interactive	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Acquisition		Application Security Testing						
SA - System and Services Acquisition	SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [at least annually (i.e., each fiscal year)] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Security and Privacy Requirements for IT Procurements].			x	x	
SA - System and Services Acquisition	SA-15(1)	Development Process, Standards, and Tools | Quality Metrics	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-15(2)	Development Process, Standards, and Tools | Security and Privacy Tracking Tools	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis	Require the developer of the system, system component, or system service to perform a criticality analysis: (a) At the following decision points in the system development life cycle: [initially at the system design/architectural design phase of the EPMR and continuously through the entire lifecycle, including O&M phase if there are significant system changes impacting criticality of system components]; and (b) At the following level of rigor: [ED approved breadth and depth of criticality analysis].			x	x	
SA - System and Services Acquisition	SA-15(5)	Development Process, Standards, and Tools | Attack Surface Reduction	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-15(6)	Development Process, Standards, and Tools | Continuous Improvement	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-15(7)	Development Process, Standards, and Tools | Automated Vulnerability Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-15(8)	Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-15(10)	Development Process, Standards, and Tools | Incident Response Plan	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-15(11)	Development Process, Standards, and Tools | Archive System or Component	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-15(12)	Development Process, Standards, and Tools | Minimize Personally Identifiable Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-16	Developer-provided Training	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [ED approved training to ensure the effectiveness of security controls implemented within ED information systems].				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-17	Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture; b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.				x	
SA - System and Services Acquisition	SA-17(1)	Developer Security and Privacy Architecture and Design | Formal Policy Model	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-17(2)	Developer Security and Privacy Architecture and Design | Security-relevant Components	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-17(3)	Developer Security and Privacy Architecture and Design | Formal Correspondence	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-17(4)	Developer Security and Privacy Architecture and Design | Informal Correspondence	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-17(5)	Developer Security and Privacy Architecture and Design |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
		Conceptually Simple Design						
SA - System and Services Acquisition	SA-17(6)	Developer Security and Privacy Architecture and Design | Structure for Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-17(7)	Developer Security and Privacy Architecture and Design | Structure for Least Privilege	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-17(8)	Developer Security and Privacy Architecture and Design | Orchestration	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-17(9)	Developer Security and Privacy Architecture and Design | Design Diversity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-20	Customized Development of Critical Components	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SA - System and Services Acquisition	SA-21	Developer Screening	Require that the developer of [any information system, component, or service where the developer needs direct access to the ED managed environment]: a. Has appropriate access authorizations as determined by assigned [Information System Owner (ISO) and ISSO]; and b. Satisfies the following additional personnel screening criteria: [in accordance with OFO-O 5-101 and/or ED defined contractor personnel screening criteria as defined in PS-7].				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SA - System and Services Acquisition	SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components [(i)must be replaced unless extended support is obtained from either the component developer or third-party service supplier certified by the original component developer; (ii)Risk acceptance (exceptions and/or waivers) signed by the ED AO are required for continued use of unsupported system components required to satisfy mission/business needs]		x	x	x	
SA - System and Services Acquisition	SA-23	Specialization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-1	Policy and Procedures	a. 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)]: 1. [Department-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls; b. Designate an [Department Chief Information Security Officer (CISO)] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and c. Review and update the current system and communications protection: 1. Policy [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]; and 2. 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].		x	x	x	
SC - System and	SC-2	Separation of System and	Separate user functionality, including user interface services, from system management functionality.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Communications Protection		User Functionality						
SC - System and Communications Protection	SC-2(1)	Separation of System and User Functionality | Interfaces for Non-privileged Users	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-2(2)	Separation of System and User Functionality | Disassociability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-3	Security Function Isolation	Isolate security functions from nonsecurity functions.				x	
SC - System and Communications Protection	SC-3(1)	Security Function Isolation | Hardware Separation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-3(2)	Security Function Isolation | Access and Flow Control Functions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-3(3)	Security Function Isolation | Minimize Nonsecurity Functionality	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-3(4)	Security Function Isolation | Module Coupling and Cohesiveness	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-3(5)	Security Function Isolation | Layered Structures	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-4	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.			x	x	
SC - System and Communications Protection	SC-4(2)	Information in Shared System Resources | Multilevel or Periods Processing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-5	Denial-of-service Protection	a. [Protect against or limit] the effects of the following types of denial-of-service events: [including, but not limited to: tear-drop; SYN flood; Smurf (ICMP) flood; Ping flood; Ping of death; peer-to-peer attacks; and application level floods. Refer to NIST 800-61 and US CERT for additional guidance on the types of DoS events]; and b. Employ the following controls to achieve the denial-of-service objective: [ED approved security safeguards including, but not limited to boundary protection devices; increased network capacity and bandwidth; service redundancy. etc.].		x	x	x	
SC - System and Communications Protection	SC-5(1)	Denial-of-service Protection | Restrict Ability to Attack Other Systems	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communi	SC-5(2)	Denial-of-service Protection | Capacity,	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
cations Protectio n		Bandwidth, and Redundancy						
SC - System and Communi cations Protectio n	SC-5(3)	Denial-of-service Protection | Detection and Monitoring	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communi cations Protectio n	SC-6	Resource Availability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communi cations Protectio n	SC-7	Boundary Protection	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.		x	x	x	
SC - System and Communi cations Protectio n	SC-7(3)	Boundary Protection | Access Points	Limit the number of external network connections to the system.			x	x	
SC - System and Communi cations Protectio n	SC-7(4)	Boundary Protection | External Telecommunica tions Services	(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.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception [at managed interfaces; with the exception of Managed Trusted Internet Provider Services (MTIPS) and when all traffic is encrypted and authenticated using zero trust architectures.]			x	x	
SC - System and Communications Protection	SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [ED approved security safeguards, (i.e. adequately provisioned VPN)].			x	x	
SC - System and Communications Protection	SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [approved and defined internal communications traffic] to [approved and defined external networks] through authenticated proxy servers at managed interfaces.			x	x	
SC - System and Communications Protection	SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-7(10)	Boundary Protection | Prevent Exfiltration	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(12)	Boundary Protection | Host-based Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(15)	Boundary Protection | Networked Privileged Accesses	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications	SC-7(16)	Boundary Protection | Prevent Discovery of	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection		System Components						
SC - System and Communications Protection	SC-7(17)	Boundary Protection | Automated Enforcement of Protocol Formats	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(18)	Boundary Protection | Fail Secure	Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.				x	
SC - System and Communications Protection	SC-7(19)	Boundary Protection | Block Communication from Non-organizationally Configured Hosts	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(20)	Boundary Protection | Dynamic Isolation and Segregation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(21)	Boundary Protection | Isolation of System Components	Employ boundary protection mechanisms to isolate [all information system components] supporting [ED mission or business functions].				x	
SC - System and Communications Protection	SC-7(22)	Boundary Protection | Separate Subnets for Connecting to Different Security Domains	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-7(23)	Boundary Protection | Disable Sender Feedback on Protocol Validation Failure	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(24)	Boundary Protection | Personally Identifiable Information	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.	x				
SC - System and Communications Protection	SC-7(25)	Boundary Protection | Unclassified National Security System Connections	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(26)	Boundary Protection | Classified National Security System Connections	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications	SC-7(27)	Boundary Protection | Unclassified Non-national Security System Connections	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection								
SC - System and Communications Protection	SC-7(28)	Boundary Protection | Connections to Public Networks	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-7(29)	Boundary Protection | Separate Subnets to Isolate Functions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-8	Transmission Confidentiality and Integrity	Protect the [confidentiality and integrity] of transmitted information.			x	x	Include LOW security control baseline systems. All sensitive information (i.e., data) must be encrypted when at rest and in transit.
SC - System and Communications Protection	SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [prevent unauthorized disclosure of information and detect changes to information] during transmission.			x	x	Include LOW security control baseline systems. All sensitive information (i.e., data) must be encrypted when at rest and in transit.
SC - System and Communications Protection	SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications	SC-8(3)	Transmission Confidentiality and Integrity | Cryptographic Protection for	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection		Message Externals						
SC - System and Communications Protection	SC-8(4)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-8(5)	Transmission Confidentiality and Integrity | Protected Distribution System	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-10	Network Disconnect	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; network connectivity, including VPN and enterprise patching service communications/connectivity, has exceeded fifteen (15) hours, unless risk accepted by the Department] of inactivity.			x	x	
SC - System and Communications Protection	SC-11	Trusted Path	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-11(1)	Trusted Path | Irrefutable Communications Path	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-12	Cryptographic Key Establishment and Management	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 13352 and FIPS 140-2 for key generation, distribution, storage, access, and destruction].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-12(1)	Cryptographic Key Establishment and Management | Availability	Maintain availability of information in the event of the loss of cryptographic keys by users.				x	
SC - System and Communications Protection	SC-12(2)	Cryptographic Key Establishment and Management | Symmetric Keys	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-12(3)	Cryptographic Key Establishment and Management | Asymmetric Keys	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-12(6)	Cryptographic Key Establishment and Management | Physical Control of Keys	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-13	Cryptographic Protection	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 NSA-approved cryptography].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-15	Collaborative Computing Devices and Applications	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.		x	x	x	
SC - System and Communications Protection	SC-15(1)	Collaborative Computing Devices and Applications | Physical or Logical Disconnect	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-15(3)	Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-15(4)	Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-16	Transmission of Security and Privacy Attributes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-16(1)	Transmission of Security and Privacy Attributes | Integrity Verification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications	SC-16(2)	Transmission of Security and Privacy Attributes |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection		Anti-spoofing Mechanisms						
SC - System and Communications Protection	SC-16(3)	Transmission of Security and Privacy Attributes | Cryptographic Binding	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-17	Public Key Infrastructure Certificates	a. Issue public key certificates under an [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.			x	x	Explicit digital signature policy
SC - System and Communications Protection	SC-18	Mobile Code	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.			x	x	
SC - System and Communications Protection	SC-18(1)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-18(2)	Mobile Code | Acquisition, Development, and Use	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-18(3)	Mobile Code | Prevent Downloading and Execution	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-18(4)	Mobile Code | Prevent Automatic Execution	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-18(5)	Mobile Code | Allow Execution Only in Confined Environments	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-20	Secure Name/address Resolution Service (authoritative Source)	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.		x	x	x	
SC - System and Communications Protection	SC-20(2)	Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-21	Secure Name/address Resolution Service (recursive or Caching Resolver)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.		x	x	x	
SC - System and Communications Protection	SC-22	Architecture and Provisioning for Name/address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.		x	x	x	
SC - System and Communi	SC-23	Session Authenticity	Protect the authenticity of communications sessions.			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
cations Protection								
SC - System and Communications Protection	SC-23(1)	Session Authenticity | Invalidate Session Identifiers at Logout	Invalidate session identifiers upon user logout or other session termination.					
SC - System and Communications Protection	SC-23(3)	Session Authenticity | Unique System-generated Session Identifiers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-23(5)	Session Authenticity | Allowed Certificate Authorities	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-24	Fail in Known State	Fail to a [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 Information System Owner (ISO) and Information System Security Officer (ISSO)].				x	
SC - System and Communications Protection	SC-25	Thin Nodes	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-26	Decoys	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-27	Platform-independent Applications	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-28	Protection of Information at Rest	Protect the [confidentiality and integrity] of the following information at rest: [all sensitive information (i.e., data) stored either on GFE or non-GFE (contractor-owned) equipment including internal or external hard disk drives, external USB drives, shared files/folders, storage area network devices, and databases].			x	x	Include LOW security control baseline systems. All sensitive information (i.e., data) must be encrypted when at rest and in transit.
SC - System and Communications Protection	SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [GFE or non-GFE (contractor-owned) equipment including internal or external hard disk drives, external USB drives, shared files/folders, storage area network devices, and databases]: [all sensitive information].			x	x	Include LOW security control baseline systems. All sensitive information (i.e., data) must be encrypted when at rest and in transit.
SC - System and Communications Protection	SC-28(2)	Protection of Information at Rest | Offline Storage	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-28(3)	Protection of Information at Rest | Cryptographic Keys	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-29	Heterogeneity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and	SC-29(1)	Heterogeneity | Virtualization Techniques	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Communications Protection								
SC - System and Communications Protection	SC-30	Concealment and Misdirection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-30(2)	Concealment and Misdirection | Randomness	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-30(3)	Concealment and Misdirection | Change Processing and Storage Locations	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-30(4)	Concealment and Misdirection | Misleading Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-30(5)	Concealment and Misdirection | Concealment of System Components	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-31	Covert Channel Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-31(1)	Covert Channel Analysis | Test Covert Channels for Exploitability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-31(2)	Covert Channel Analysis | Maximum Bandwidth	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-31(3)	Covert Channel Analysis | Measure Bandwidth in Operational Environments	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-32	System Partitioning	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-32(1)	System Partitioning | Separate Physical Domains for Privileged Functions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-34	Non-modifiable Executable Programs	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications	SC-34(1)	Non-modifiable Executable Programs | No Writable Storage	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection								
SC - System and Communications Protection	SC-34(2)	Non-modifiable Executable Programs | Integrity Protection on Read-only Media	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-35	External Malicious Code Identification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-36	Distributed Processing and Storage	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-36(1)	Distributed Processing and Storage | Polling Techniques	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-36(2)	Distributed Processing and Storage | Synchronization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-37	Out-of-band Channels	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-37(1)	Out-of-band Channels | Ensure Delivery and Transmission	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-38	Operations Security	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.		x	x	x	
SC - System and Communications Protection	SC-39(1)	Process Isolation | Hardware Separation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-39(2)	Process Isolation | Separate Execution Domain Per Thread	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-40	Wireless Link Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications	SC-40(1)	Wireless Link Protection | Electromagnetic Interference	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection								
SC - System and Communications Protection	SC-40(2)	Wireless Link Protection | Reduce Detection Potential	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-40(3)	Wireless Link Protection | Imitative or Manipulative Communications Deception	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-40(4)	Wireless Link Protection | Signal Parameter Identification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-41	Port and I/O Device Access	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-42	Sensor Capability and Data	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-42(1)	Sensor Capability and Data | Reporting to Authorized Individuals or Roles	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-42(2)	Sensor Capability and Data | Authorized Use	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-42(4)	Sensor Capability and Data | Notice of Collection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-42(5)	Sensor Capability and Data | Collection Minimization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-43	Usage Restrictions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-44	Detonation Chambers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications	SC-45	System Time Synchronization	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Protection								
SC - System and Communications Protection	SC-45(1)	System Time Synchronization | Synchronization with Authoritative Time Source	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-45(2)	System Time Synchronization | Secondary Authoritative Time Source	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-46	Cross Domain Policy Enforcement	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-47	Alternate Communications Paths	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-48	Sensor Relocation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-48(1)	Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SC - System and Communications Protection	SC-49	Hardware-enforced Separation and Policy Enforcement	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-50	Software-enforced Separation and Policy Enforcement	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SC - System and Communications Protection	SC-51	Hardware-based Protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-1	Policy and Procedures	a. 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)]: 1. [Department-level] system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls; b. Designate an [Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP)] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and c. Review and update the current system and information integrity: 1. Policy [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]; and 2. 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].	x	x	x	x	
SI - System and Information Integrity	SI-2	Flaw Remediation	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [a timeline in accordance with Department policies and standards, the criticality of the updates, risk to the Department, prioritization of resources, and as required to comply with CISA/OMB requirements for flaw remediation and patching] of the release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process.		x	x	x	
SI - System and Information Integrity	SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [ED approved automated mechanisms] [at least monthly].			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-2(4)	Flaw Remediation | Automated Patch Management Tools	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-2(5)	Flaw Remediation | Automatic Software and Firmware Updates	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-2(6)	Flaw Remediation | Removal of Previous Versions of Software and Firmware	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-3		a. Implement [signature based and non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [at least weekly] and real-time scans of files from external sources at [endpoint and network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Block or quarantine malicious code]; and send alert to [the EDSOC and when feasible, to system administrators or other personnel assigned to serve in incident response roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.		x	x	x	
SI - System and Information Integrity	SI-3(4)	Malicious Code Protection | Updates Only by Privileged Users	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-3(6)	Malicious Code Protection | Testing and Verification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-3(8)	Malicious Code Protection | Detect Unauthorized Commands	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-3(10)	Malicious Code Protection | Malicious Code Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [ED IT/Cybersecurity monitoring objectives as defined in ED Information Security Continuous Monitoring Roadmap]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [ED approved security safeguards including but not limited to: continuous monitoring, vulnerability scans, malicious code protection mechanisms, intrusion detection or prevention mechanisms, and/or boundary protection devices such as firewalls, gateways, and routers]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [ED approved information system monitoring output] to [the Information System Owner (ISO) and Information System Security Officer (ISSO) who distribute the information to other personnel with system administration, monitoring, and/or security responsibilities] [as needed and in accordance with ED policy].		x	x	x	
SI - System and Information Integrity	SI-4(1)	System Monitoring | System-wide Intrusion Detection System	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.			x	x	
SI - System and Information Integrity	SI-4(3)	System Monitoring | Automated Tool and Mechanism Integration	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [continuously] for [unusual or unauthorized activities or conditions].			x	x	
SI - System and Information Integrity	SI-4(5)	System Monitoring | System-generated Alerts	Alert [personnel with incident response, system administration, monitoring, and/or security responsibilities] when the following system-generated indications of compromise or potential compromise occur: [ED defined list of compromised indicators or indications that the system's integrity has been breached including, but not limited to compromise indicators may include but shall not be limited to the following: - Protected system files or directories have been modified without notification from the appropriate change/configuration management channels. - System performance indicates resource consumption that is inconsistent with expected operating conditions. - Auditing functionality has been disabled or modified to reduce audit visibility. - Audit or log records have been deleted or modified without explanation. - The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition. - Resource or service requests are initiated from clients that are outside of the expected client membership set. - The system reports failed logins or password changes for administrative or key service accounts. - Processes and services are running that are outside of the baseline system profile. - Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose].			x	x	
SI - System and Information Integrity	SI-4(7)	System Monitoring | Automated Response to Suspicious Events	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(9)	System Monitoring | Testing of Monitoring Tools and Mechanisms	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(10)	System Monitoring | Visibility of Encrypted Communications	Make provisions so that [ED-approved encrypted communications traffic] is visible to [ED-approved system monitoring tools and mechanisms].				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(12)	System Monitoring | Automated Organization-generated Alerts	Alert [personnel with incident response, system administration, monitoring, and/or security responsibilities including but not limited to EDSOC and System Administrators] using [ED-authorized automated mechanisms, including e-mail] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [activities that trigger alerts].				x	
SI - System and Information Integrity	SI-4(13)	System Monitoring | Analyze Traffic and Event Patterns	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(14)	System Monitoring | Wireless Intrusion Detection	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.				x	
SI - System and Information Integrity	SI-4(15)	System Monitoring | Wireless to Wireline Communications	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(16)	System Monitoring | Correlate Monitoring Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(17)	System Monitoring | Integrated Situational Awareness	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati	SI-4(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
on Integrity								
SI - System and Information Integrity	SI-4(19)	System Monitoring | Risk for Individuals	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(20)	System Monitoring | Privileged Users	Implement the following additional monitoring of privileged users: [ED defined additional monitoring including but not limited to : Privileged Account Management (PAM) sufficient to provide nonrepudiation for administrative actions (when technically feasible); device compliance authorization; locational account lockouts; statistical and analytical review of privileged user activity; multifactor authentication (MFA) misuse; naming policy compliance; date and time (normal operation time); and other logging requirements noted in Office of Management and Budget (OMB) Memorandum M-21-31, dated August 27, 2021 or successor as appropriate].				x	
SI - System and Information Integrity	SI-4(21)	System Monitoring | Probationary Periods	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(22)	System Monitoring | Unauthorized Network Services	(a) Detect network services that have not been authorized or approved by [ED authorization or approval processes]; and (b) [Audit; and Alert [personnel with responsibilities for performing system and or network monitoring] when detected.				x	
SI - System and Information Integrity	SI-4(23)	System Monitoring | Host-based Devices	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-4(24)	System Monitoring | Indicators of Compromise	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati	SI-4(25)	System Monitoring | Optimize Network Traffic Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
on Integrity								
SI - System and Information Integrity	SI-5	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [EDSOC (e.g., ED alerts, advisories and directives as well as alerts and advisories received by ED from the Cybersecurity and Infrastructure Security Agency (CISA), Office of Management and Budget, etc.) as well as from external organizations, when appropriate and available, such as supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [all staff with system administration, monitoring, and/or security responsibilities including but not limited to Principal Offices, Information System Owner (ISO) and Information System Security Officer (ISSO)]; and d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.		x	x	x	
SI - System and Information Integrity	SI-5(1)	Security Alerts, Advisories, and Directives | Automated Alerts and Advisories	Broadcast security alert and advisory information throughout the organization using [ED approved automated mechanisms to include but not be limited to: email].				x	
SI - System and Information Integrity	SI-6	Security and Privacy Function Verification	a. Verify the correct operation of [security and privacy functions]; b. Perform the verification of the functions specified in SI-6a [on system startup, restart; and/or abort; upon command by user with appropriate privilege; every 7 days]; c. Alert [designated ED personnel with information security and/or privacy responsibilities (e.g., System administrators, ISSO)] to failed security and privacy verification tests; and d. [Shut down or restart the information system, and notifies system administrators, security personnel and/or privacy personnel] when anomalies are discovered.				x	
SI - System and Information Integrity	SI-6(2)	Security and Privacy Function Verification | Automation Support for Distributed Testing	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-6(3)	Security and Privacy Function Verification | Report Verification Results	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-7	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [ED-authorized software, firmware, and information including but not limited to: system kernels, drivers, firmware, (e.g., BIOS) software (e.g., OS, applications, middleware) and security attributes]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [system administrators]].			x	x	
SI - System and Information Integrity	SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	Perform an integrity check of [ED software, firmware, and information within ED information systems] [at startup or restart; at the occurrence of configuration changes or security-relevant events; the identification of a new threat to which the information system is susceptible; installation of new hardware] [at least monthly].			x	x	
SI - System and Information Integrity	SI-7(2)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations	Employ automated tools that provide notification to [system administrators and other personnel with responsibilities for system/network monitoring] upon discovering discrepancies during integrity verification.				x	
SI - System and Information Integrity	SI-7(3)	Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-7(5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations	Automatically [initiate ED Approved incident response process] when integrity violations are discovered.				x	
SI - System and Informati	SI-7(6)	Software, Firmware, and Information Integrity |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
on Integrity		Cryptographic Protection						
SI - System and Informati on Integrity	SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [changes to established configuration settings and unauthorized elevation of system privileges].			X	X	
SI - System and Informati on Integrity	SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-7(9)	Software, Firmware, and Information Integrity | Verify Boot Process	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-7(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-7(12)	Software, Firmware, and Information Integrity | Integrity Verification	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-7(15)	Software, Firmware, and Information Integrity | Code Authentication	Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [ED-approved software or firmware components].				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-7(16)	Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-7(17)	Software, Firmware, and Information Integrity | Runtime Application Self-protection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-8	Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.			x	x	All second-level agency domains must have valid SPF/DMARC records, with a policy of "reject" for second-level domains and mail-sending hosts
SI - System and Information Integrity	SI-8(2)	Spam Protection | Automatic Updates	Automatically update spam protection mechanisms [daily or when updates are made available from product vendor].			X	X	
SI - System and Information Integrity	SI-8(3)	Spam Protection | Continuous Learning Capability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-10	Information Input Validation	Check the validity of the following information inputs: [character set, length, numerical range, and acceptable values to verify that inputs match specified definitions for format and content as it relates to: both manual user inputs and automated inputs]			x	x	
SI - System and Informati	SI-10(1)	Information Input Validation | Manual	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
on Integrity		Override Capability						
SI - System and Informati on Integrity	SI-10(2)	Information Input Validation | Review and Resolve Errors	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-10(3)	Information Input Validation | Predictable Behavior	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-10(4)	Information Input Validation | Timing Interactions	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-10(5)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-10(6)	Information Input Validation | Injection Prevention	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-11	Error Handling	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and b. Reveal error messages only to [authorized ED personnel].			x	x	
SI - System and Informati on Integrity	SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	x	x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [approved elements of personally identifiable information].	x				
SI - System and Information Integrity	SI-12(2)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [approved techniques such as collecting the minimum identity data needed; de-identifying data as soon as possible after collection and/or separating data elements into a coded data set and an identity-only data set; using encryption if identifiable information is: (1) stored on a networked computer or device; (2) transmitted over a network; and/or (3) stored on a removable medium (e.g., laptop computer or a USB flash drive); and limiting access to personally identifiable information].	x				
SI - System and Information Integrity	SI-12(3)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [in accordance with the current version of NIST SP 800-88].	x				
SI - System and Information Integrity	SI-13	Predictable Failure Prevention	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-13(1)	Predictable Failure Prevention | Transferring Component Responsibilities	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-13(3)	Predictable Failure Prevention | Manual Transfer Between Components	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati	SI-13(4)	Predictable Failure Prevention | Standby Component	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
on Integrity		Installation and Notification						
SI - System and Informati on Integrity	SI-13(5)	Predictable Failure Prevention | Failover Capability	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-14	Non-persistence	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-14(1)	Non-persistence | Refresh from Trusted Sources	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-14(2)	Non-persistence | Non-persistent Information	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-14(3)	Non-persistence | Non-persistent Connectivity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-15	Information Output Filtering	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Informati on Integrity	SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code execution: [ED approved security safeguards to include but not limited to the use of either hardware or software based data execution prevention and address space layout randomization].			x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-17	Fail-safe Procedures	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-18	Personally Identifiable Information Quality Operations	a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [at least annually (i.e., each fiscal year)]; and b. Correct or delete inaccurate or outdated personally identifiable information.	x				
SI - System and Information Integrity	SI-18(1)	Personally Identifiable Information Quality Operations | Automation Support	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-18(2)	Personally Identifiable Information Quality Operations | Data Tags	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-18(3)	Personally Identifiable Information Quality Operations | Collection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-18(4)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	x				
SI - System and Information Integrity	SI-18(5)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-19	De-identification	a. Remove the following elements of personally identifiable information from datasets: [PII and Sensitive PII]; and b. Evaluate [at least annually (i.e., each fiscal year] for effectiveness of de-identification.	x				
SI - System and Information Integrity	SI-19(1)	De-identification | Collection	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-19(2)	De-identification | Archiving	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-19(3)	De-identification | Release	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-19(4)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-19(5)	De-identification | Statistical Disclosure Control	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-19(6)	De-identification | Differential Privacy	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SI - System and Information Integrity	SI-19(7)	De-identification | Validated Algorithms and Software	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-19(8)	De-identification | Motivated Intruder	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-20	Tainting	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-21	Information Refresh	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-22	Information Diversity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SI - System and Information Integrity	SI-23	Information Fragmentation	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SR - Supply Chain Risk Managem ent	SR-1	Policy and Procedures	a. 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)]: 1. [Department-level] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b. Designate a [Department Chief Information Security Officer (CISO)] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 1. Policy [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]; and 2. 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 Department 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].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SR - Supply Chain Risk Managem ent	SR-2	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [within the Department's FISMA inventory]; b. Review and update the supply chain risk management plan [annually (i.e., each fiscal year)] or as required, to address threat, organizational or environmental changes; and c. Protect the supply chain risk management plan from unauthorized disclosure and modification.		x	x	x	
SR - Supply Chain Risk Managem ent	SR-2(1)	Supply Chain Risk Management Plan | Establish SCRM Team	Establish a supply chain risk management team consisting of [SCRM Senior Agency Official, ICT SCRM Program Manager, ICT SCRM Team, CISO, CIO, ISSO, ISO, CO and COR] to lead and support the following SCRM activities: [1. Frame ICT SCRM risks based upon ED risk tolerance levels and multi-tiered risk management roles and responsibilities at the organizational, mission, and information system level; 2. Assess ICT SCRM risks based upon NIST SP 800-30 (as amended), CNSSI 4009, NIST SP 800-53, Rev. 5 (RA-3), and other Department assessment methodologies; 3. Respond to ICT SCRM risks by following the ED POA&M process; 4. Monitor ICT SCRM risks in accordance with NIST SP 800-137 guidance, Department risk tolerance levels, and the re-assessment preconditions defined by the Department].		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SR - Supply Chain Risk Managem ent	SR-3	Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Department systems and their components] in coordination with [Department enterprise and mission stakeholders defined within the ICT SCRM Roadmap]; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Department organizationally defined controls detailed in the ED ICT SCRM Strategy]; and c. Document the selected and implemented supply chain processes and controls in [System Security Plans.]		x	x	x	
SR - Supply Chain Risk Managem ent	SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SR - Supply Chain Risk	SR-3(2)	Supply Chain Controls and Processes |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Management		Limitation of Harm						
SR - Supply Chain Risk Management	SR-3(3)	Supply Chain Controls and Processes | Sub-tier Flow Down	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems; supply chain overlay applies.					Tier 1 (prime) contractors include processes within risk management plans and SLAs to ensure sub-tier contractors implement SR-3b, SR-5, and SR-8 controls.
SR - Supply Chain Risk Management	SR-4	Provenance	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems; supply chain overlay applies.					All software supporting FIPS-199 High systems must have software bill of materials (SBOM) documentation. Documentation must be reported to the ICT SCRM Team.
SR - Supply Chain Risk Management	SR-4(1)	Provenance | Identity	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems; supply chain overlay applies.					Tier 1 (prime) suppliers for FIPS-199 High systems must maintain visibility into supply chain activities. Supplier self-attestation to ED is required and periodic supply chain risk assessments will be used to validate control implementation.
SR - Supply Chain Risk Management	SR-4(2)	Provenance | Track and Trace	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems; supply chain overlay applies.					All hardware supporting FIPS 199 High systems must be labeled using serial numbers or tagged using radiofrequency identification tags. Shipping delays or lost inventory must

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
								be reported to the ICT SCRM Team.
SR - Supply Chain Risk Managem ent	SR-4(3)	Provenance | Validate as Genuine and Not Altered	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SR - Supply Chain Risk Managem ent	SR-4(4)	Provenance | Supply Chain Integrity — Pedigree	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SR - Supply Chain Risk Managem ent	SR-5	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [ICT vendor and supplier attestation of conformance to NIST SP 800-161 (as amended) C-SCRM practices, ICT vendor and supplier self attestation of compliance with NDAA Section 889, Part B, ICT vendor and supplier reporting of supply chain cyber incidents to EDSOC, ICT vendor and supplier support in complying with EO 14028, and ICT vendor and supplier joint training with ED ICT SCRM stakeholders.]		x	x	x	
SR - Supply Chain Risk	SR-5(1)	Acquisition Strategies, Tools, and Methods |	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
Management		Adequate Supply						
SR - Supply Chain Risk Management	SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems; supply chain overlay applies.					Software: Software Bill of Materials (SBOM) will be evaluated to prior to use; Hardware: Physical inspection of hardware deliveries will be conducted prior to use. Physical inspection results will be submitted to the ICT SCRM Team.
SR - Supply Chain Risk Management	SR-6	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [annually (i.e., each fiscal year) or upon the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and Department 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].			x	x	
SR - Supply Chain Risk Management	SR-6(1)	Supplier Assessments and Reviews | Testing and Analysis	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems; supply chain overlay applies.					Supplier risk assessments will be performed in accordance with the ICT supply chain risk assessment schedule.
SR - Supply Chain Risk Management	SR-7	Supply Chain Operations Security	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SR - Supply Chain Risk Managem ent	SR-8	Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [notification of supply chain compromises; results of assessments or audits; [all instances of IT system compromises impacting Department systems.]		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SR - Supply Chain Risk Managem ent	SR-9	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.				x	
SR - Supply Chain Risk Managem ent	SR-9(1)	Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.				x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SR - Supply Chain Risk Managem ent	SR-10	Inspection of Systems or Components	Inspect the following systems or system components [Moderate and High systems, annually (i.e., each fiscal year), or upon indications of need for inspection by the ICT SCRM Team. Asset managers will inspect deliverables prior to use and consult with the ICT SCRM Team as needed] to detect tampering: [in Moderate and High systems; the inspection of systems or components for tampering will address physical and logical tampering, inspections of packaging modifications, review of delivery invoices, and other physical properties that indicate a potential compromise. Software hashes will be inspected and the SBOM reviewed prior to use.]		x	x	x	
SR - Supply Chain Risk Managem ent	SR-11	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit system components to [the EDSOC, ICT SCRM Team, and ISSO for further action].		x	x	x	
SR - Supply Chain Risk Managem ent	SR-11(1)	Component Authenticity | Anti-counterfeit Training	Train [ICT SCRM Team, hardware and software asset managers and others responsible for hardware and software inventories] to detect counterfeit system components (including hardware, software, and firmware).		x	x	x	

Control Family	Control Identifier	Control (or Control Enhancement) Name	ED Control Requirement	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	ED Specific Control Overlay (Requirements not in 800-53 baseline controls)
SR - Supply Chain Risk Managem ent	SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [all components].		x	x	x	
SR - Supply Chain Risk Managem ent	SR-11(3)	Component Authenticity | Anti-counterfeit Scanning	Not applicable to Privacy Baseline or Security Control Baseline for L-M-H systems					
SR - Supply Chain Risk Managem ent	SR-12	Component Disposal	Dispose of [data, documentation (paper-based and digital files), tools, and system components throughout the system development lifecycle] using the following techniques and methods: [Enterprise Review Board Checklist, System Retirement Plan, and the current version of NIST SP 800-88, Guidelines for Media Sanitization].		x	x	x	