Information Technology (IT) System Access Control (AC) Standard

February 10, 2023

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

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

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.02.09 17:34:01 -05'00'

Steven Hernandez

Director, IAS/Chief Information Security Officer (CISO)

Revision History

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

Table 1: Revision History

Version	Date	Summary of Changes
1.0	12/22/2021	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/14/2022	Update to incorporate feedback from Information Assurance Services (IAS), Governance, Risk and Policy (GRP) Team.
1.2	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with EO 14028.
1.3	2/11/2022	Update to AC-2(j)
1.4	2/10/2023	Annual review. Clean up formatting and numbering throughout and update broken links. Add footnote to HVA control reference in Section 2. Updated AC-2c and AC-2d to provide clarity. Added control overlay to include AC-2(3), AC-5, and AC-6 to the ED Low system baseline. Added control overlay AC-2(2). Updated AC-10 and AC-19(5). Added AC-20(3) control overlays ED-01 through ED-04.

Contents

1 INTRODUCTION

This governance document establishes Department information technology (IT) system access controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

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

1.2 Scope

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

2 STANDARDS

The Department standards for IT system access controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for

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

Department information systems, a FIPS 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay5 issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

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

2.1 AC-1 Policy and Procedures (P, L, M, H)

Develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems/services operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a department-level access control policy (e.g., this document) that:

(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as OCIO: 3-112/ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT system access control policy.

Review and update the 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

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

technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

The Office of the Chief Information Officer (OCIO), Information Assurance Services (IAS) manage the development, documentation, and dissemination of the Department-level IT system access control standard operating procedures in support of this policy standard. IAS Branch Chiefs shall review these access control 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.

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

2.2 AC-2 Account Management (L, M, H and Control Overlay)

a. Define and document the types of accounts allowed and specifically prohibited for use within the system.

b. Assign account managers.

c. Require ISO and ISSO to document recommended prerequisites and criteria (based on defined user role(s) matrix in the System Security Plan (SSP) System Description Narrative: Types of Users) and require implementation of these prerequisites and criteria for group and role membership.

d. Specify:

    1. Authorized users of the system.

    2. Group and role membership.

    3. Access authorizations (i.e., privileges) and the following attributes as defined in the user role(s) matrix in SSP System Description Narrative: User Types: Internal or External; Privileged (P), Non-Privileged (NP), or No Logical Access (NLA);

Sensitivity Level[6] in accordance with control PS-2; Authorized Privileges; and Functions Performed for each account.

e. Require approvals by ISO, ISSO, or assigned delegate for requests to create accounts.

f. Create, enable, modify, disable, and remove accounts in accordance with least privilege and separation of duties, and Department policies and supporting standards, including the standards within this document.

g. Monitor the use of accounts.

h. Notify account managers 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 monthly for HVAs and High impact systems and quarterly for Moderate and Low impact systems. Based upon the review, modify, or remove accounts, as necessary, to correctly reflect organizational mission and business need. Not applicable to cloud service providers or Shared Services.

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group.

l. Align account management processes with personnel termination and transfer process.

Control Overlay AC-2 ED-01 (L, M, H): Uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.

[6] Position Sensitivity And Risk (opm.gov)

Control Overlay AC-2 ED-02 (L, M, H): Follow privileged access management principles for network-based administration of EO-critical software and EO-critical software platforms by requiring unique identification of each administrator.

2.2.1 AC-2(1) Account Management | Automated System Account Management (M, H)

Support the management of system accounts using internal system functions, ED Identity, Credential, and Access Management (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 ISO and ISSO, when functionality is available.

2.2.2 AC-2(2) Account Management | Automated Temporary and Emergency Account Management (M, H)

Automatically disable temporary and emergency accounts after identification that the temporary/emergency access is no longer required, not to exceed ninety (90) days after the creation date.

Control Overlay AC-2(2) ED-01 (L, M, H): Document, approve and govern emergency/break glass accounts required to support administration of Department mission critical infrastructure.

2.2.3 AC-2(3) Account Management | Disable Accounts (M, H)

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 ninety (90) days for Moderate systems and 30 days for High systems and HVAs. If no automated capability is available, manual methods must be implemented and documented in the SSP. ISSOs are responsible for ensuring inactive accounts are disabled if the system cannot do so automatically.

Control Overlay AC-2(3) ED-01 (L): 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 ninety (90) days for Low systems. If no automated capability is available, manual methods must be implemented and documented in the SSP. ISSOs are responsible for ensuring inactive accounts are disabled if the system cannot do so automatically.

2.2.4 AC-2(4) Account Management | Automated Audit Actions (M, H)

Automatically audit account creation, modification, enabling, disabling, and removal actions.

2.2.5 AC-2(5) Account Management | Inactivity Logout (M, H)

Require that users log out when they expect to be inactive for more than 12 hours.

2.2.6 AC-2(11) Account Management | Usage Conditions (H)

Enforce 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 ISO for privileged user, temporary and emergency accounts.

2.2.7 AC-2(12) Account Management | Account Monitoring for Atypical Usage (H)

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 ED Security Operations Center (EDSOC) and ISSO.

2.2.8 AC-2(13) Account Management | Disable Accounts for High-risk Individuals (M, H)

Disable accounts of individuals within twenty-four (24) hours of discovery of a security incident reported to or under investigation by the EDSOC. Accounts can be directed to be disabled by the CIO/CISO/ED Information System Security Manager (ISSM)/ISSO/ISO/Contracting Officer’s Representative (COR)/EDSOC in reference to a security incident. If automated disabling capability is unavailable, manual methods must be implemented and documented in the SSP. ISSOs are responsible for ensuring inactive accounts are disabled.

2.3 AC-3 Access Enforcement (L, M, H)

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

2.3.1 AC-3(14) Access Enforcement | Individual Access (P)

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 Office of General Counsel (OGC) consulted to determine appropriate mechanisms and access rights or limitations.

2.4 AC-4 Information Flow Enforcement (M, H)

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).

2.4.1 AC-4(4) Information Flow Enforcement | Flow Control of Encrypted Information (H)

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.

2.5 AC-5 Separation of Duties (M, H and Control Overlay)

a. Identify and document within the system description narrative, all system user roles, privileges, and duties assigned to each role, the specific duties and privileges that each role cannot perform, and rationale for why they are incompatible; and
b. Define system access authorizations to support separation of duties.

Control Overlay AC-5 ED-01 (M, H): Separate duties so that critical IT functions are segregated to prevent any one person from having the authority or ability to harm or circumvent normal checks and balances of a development or an operational system or the services it provides, whether by accident, omission, or intentional act.

Control Overlay AC-5 ED-02 (M, H): Consider and document the potential for fraudulent activity in assigning and reviewing system access privileges.

Control Overlay AC-5 ED-03 (M, H): Determine assignment of roles by ISOs and designees to ensure:

a. At least two people are involved within each process or sub-process

b. Two people are involved in certain controls, where necessary (i.e., at times a single control may be split into activities that are assigned to different individuals)

Control Overlay AC-5 ED-04 (M, H): Ensure system development roles for financial systems categorized as HVAs are distinctly segregated from production environments. Per OFO: 1-103 / ACSD-OFO-003, *Financial Management*, a financial system is an information system comprised of one or more applications that are used for any of the following:

a. Collecting, processing, maintaining, transmitting, and reporting data about financial events;

b. Supporting financial planning or budgeting activities;

c. Accumulating and reporting cost information; or

d. Supporting the preparation of financial statements.

Control Overlay AC-5 ED-05 (M, H): Ensure the following incompatible responsibilities are separated for financial systems:

a. Initiation of a transaction vs. approval of the same transaction

b. Updating of vendor/employee records vs. approval of financial transactions related to that vendor/employee

c. Processing of transactions vs. authorization of access to systems/applications.

Control Overlay AC-5 ED-06 (M, H): Establish mitigating controls in instances in which it is impractical to have meaningful separation of duties due to limited staff and ensure these controls are rigorously documented and followed. In such cases, direct managerial involvement provides a strong deterrent to potential conflicting activities/interests. Examples of such involvement include:

a. Rotation of duties among personnel

b. Increased hands-on supervision

c. Enforced vacations

d. Having a manager perform one aspect of the transaction (e.g., approving invoices, etc.)

e. Active review by management of financial data and reports (e.g., reconciliations, voucher status report, appropriation status reports)

f. A detailed management review of activities involving finances, inventory, and other assets must be required as a compensating control activity.

g. Increased frequency of audit log review, especially for those logs generated from privileged user activities.

Control Overlay AC-5 ED-07 (L):

a. Identify and document within the system description narrative, all system user roles, privileges, and duties assigned to each role, the specific duties and privileges that each role cannot perform, and rationale for why they are incompatible; and

b. Define system access authorizations to support separation of duties.

2.6 AC-6 Least Privilege (M, H and Control Overlay)

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 task.

Control Overlay AC-6 ED-01 (L, M, H): Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.

Control Overlay AC-6 ED-02 (L): 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 task.

2.6.1 AC-6(1) Least Privilege | Authorize Access to Security Functions (M, H)

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:

    1. Establishing system accounts, configuring access authorizations (i.e., permissions, privileges);
    2. Setting/modifying audit logs and auditing behavior;
    3. Setting/modifying boundary protection system rules;
    4. Configuring/modifying access authorizations (i.e., permissions, privileges);
    5. Setting/modifying authentication parameters; and
    6. 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.

2.6.2 AC-6(2) Least Privilege | Non-privileged Access for Nonsecurity Functions (M, H)

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.

2.6.3 AC-6(3) Least Privilege | Network Access to Privileged Commands (H)

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 ISO, ISSO, and or the AO, based upon an assessment of risk and document the rationale for such access in the security plan for the system.

2.6.4 AC-6(5) Least Privilege | Privileged Accounts (M, H)

Restrict privileged accounts on the system to individuals, services and systems/machines approved by the ISO, ISSO, and/or the AO based upon an assessment of risk.

2.6.5 AC-6(7) Least Privilege | Review of User Privileges (M, H and Control Overlay)

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.

Control Overlay AC-6(7) ED-01 (L): Quarterly for Low impact systems, review the privileges assigned to all privileged roles and users to validate the need for such privileges. Based upon the review, reassign, or remove privileges, if necessary, to correctly reflect organizational mission and business need.

2.6.6 AC-6(9) Least Privilege | Log Use of Privileged Functions (M, H)

Log the execution of privileged functions.

2.6.7 AC-6(10) Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions (M, H)

Prevent non-privileged users from executing privileged functions.

2.7 AC-7 Unsuccessful Logon Attempts (L, M, H)

a. Enforce a limit of three (3) consecutive invalid logon attempts by a user during a thirty (30) minute time period with system accounts locked immediately upon any unsuccessful attempt to login; and
b. Automatically lock the account or node for thirty (30) minutes, unless the user contacts the Help Desk to manually unlock the account during the thirty (30) minute period. For system accounts and systems unable to set the thirty (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 administrator can re-enable it.

2.8 AC-8 System Use Notification (L, M, H and Control Overlay)

Except for Institute of Education Sciences' websites that adhere to the Education Science Reform Act[7], all Principal Office systems must:

a. Display the Department's approved system use notification message or banner (see Appendix B) 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;

[7] Education Sciences Reform Public Law 107-279

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.
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.

Control Overlay AC-8 ED-01 (L, M, H): The System Use Notification or Warning Banner shall be documented and implemented before an Authorization to Operate (ATO) is issued or if during change management a new site or existing site is changed that would necessitate the re-validation that the banner is still implemented and presented to users of internet-accessible production web applications and ED websites.

2.9 AC-10 Concurrent Session Control (H)

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 ISSO.

2.10 AC-11 Device Lock (M, H)

a. Prevent further access to the system by initiating a device lock after fifteen (15) 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.

2.10.1 AC-11(1) Device Lock | Pattern-hiding Displays (M, H)

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

2.11 AC-12 Session Termination (M, H)

Automatically terminate a user session after:

a. Zero trust architecture standards, guidance, and memorandums from CISA, OMB or NIST;
b. Targeted responses to certain types of incidents;
c. Time-of-day restrictions on system use, if implemented;

d. Thirty (30) minutes of session inactivity; and
e. 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.

2.12 AC-14 Permitted Actions Without Identification or Authentication (L, M, H)

a. Identify specific actions based upon an assessment of risk 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.

2.13 AC-17 Remote Access (L, M, H)

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.

2.13.1 AC-17(1) Remote Access | Monitoring and Control (M, H)

Employ automated mechanisms to monitor and control remote access methods.

2.13.2 AC-17(2) Remote Access | Protection of Confidentiality and Integrity Using Encryption (M, H)

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

2.13.3 AC-17(3) Remote Access | Managed Access Control Points (M, H)

Route remote accesses through authorized and managed network access control points.

2.13.4 AC-17(4) Remote Access | Privileged Commands and Access (M, H)

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.

2.14 AC-18 Wireless Access (L, M, H)

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.

2.14.1 AC-18(1) Wireless Access | Authentication and Encryption (M, H)

Protect wireless access to the system using authentication of users and devices and FIPS validated encryption.

2.14.2 AC-18(3) Wireless Access | Disable Wireless Networking (M, H)

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

2.14.3 AC-18(4) Wireless Access | Restrict Configurations by Users (H)

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

2.14.4 AC-18(5) Wireless Access | Antennas and Transmission Power Levels (H)

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.

2.15 AC-19 Access Control for Mobile Devices (L, M, H)

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.

2.15.1 AC-19(5) Access Control for Mobile Devices | Full Device or Container-based Encryption (M, H)

Employ full device encryption whenever possible, or with written AO authorization, container encryption when full device is not possible to protect the confidentiality and integrity of information on ED-approved and authorized mobile devices and services.

2.16 AC-20 Use of External Systems (L, M, H)

a. Establish, maintain and monitor Interconnection Security Agreements (ISAs), Inter Agency Agreements (IAA) and other agreements with external agencies per NIST SP 800-47 and ED policies and standards including OPEPD: 1-101/ACSD-OFO-051, *Interagency Agreements* and OCIO: 3-113/ACSD-OCIO-002, *Controlled Unclassified Information Program*; 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

b. Prohibit the use of external systems not covered by a current ISA, IAA, or other agreements with external agencies.

2.16.1 AC-20(1) Use of External Systems | Limits on Authorized Use (M, H)

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 Department's security and privacy policies and system specific security and privacy plans; or

b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

2.16.2 AC-20(2) Use of External Systems | Portable Storage Devices — Restricted Use (M, H)

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.

2.16.3 AC-20(3) Use of External Systems | Non-Organizationally Owned Systems – Restricted Use (Control Overlay)

Not applicable to Privacy Baseline or Security Control Baseline for Low, Moderate, or High systems; control overlays apply.

Control Overlay AC-20(3) ED-01 (L, M, H): Prohibit conducting official ED business using personal or corporate email accounts if an official Department email account has been assigned.

Control Overlay AC-20(3) ED-02 (L, M, H): Prohibit configuring Department email accounts to auto-forward to non-ED.gov email addresses, by an email administrator or an end user, without formal approval by the Office of the Chief Information Officer (OCIO), Enterprise Technology Services (ETS-ISS).

Control Overlay AC-20(3) ED-03 (L, M, H): Prohibit the use of any external system or device that is not ED owned or authorized including the use of personally owned or corporate-owned systems and services unless specifically authorized as an exception by the EPMR/EA (TI).

2.17 AC-21 Information Sharing (M, H)

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.

2.18 AC-22 Publicly Accessible Content (L, M, H)

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.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

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

APPENDIX A: ACRONYMS

Table 2: Acronym List

ACS	Administrative Communications System
AO	Authorizing Official
ATO	Authorization to Operate
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COR	Contracting Officer's Representative
CSAM	Cyber Security Assessment and Management tool
DHS	Department of Homeland Security
ED	Department of Education
EDSOC	ED Security Operations Center
EO	Executive Order
FIPS	Federal Information Processing Standard
GRP	Governance, Risk and Policy
HVA	High Value Asset
IAA	Inter Agency Agreement
IAS	Information Assurance Services
ISA	Interconnection Security Agreement
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
NDA	Non-disclosure Agreements
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OFO	Office of Finance and Operations
OMB	Office of Management and Budget

RAF	**Risk Acceptance Form**
SAML	**Security Assertion Markup Language**
SAOP	**Senior Agency Official for Privacy**
SSP	**System Security Plan**
VPN	**Virtual Private Network**
WS	**Web Service**
XACML	**Extensible Access Control Markup Language**

APPENDIX B: BASELINE CONTROL PARAMETER SUMMARY

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

Table 3: Summary of Baseline Controls

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
AC-1	Policy and Procedures	x	x	x	x	PR.AC, DE.DP, GV.PO-P, GV.MT-P, CT.PO-P, PR.AC-P	PR.AC-3, PR.AC-4, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CT.PO-P2, CT.PO-P3, PR.AC-P3, PR.AC-P4
AC-2	Account Management		x	x	x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-2(1)	Account Management | Automated System Account Management			x	x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-2(2)	Account Management | Automated Temporary and Emergency Account Management			x	x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-2(3)	Account Management | Disable Accounts			x	x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-2(4)	Account Management | Automated Audit Actions			x	x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
AC-2(5)	Account Management | Inactivity Logout			x	x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
*AC-2(6)	Account Management | Dynamic Privilege Management					PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
*AC-2(7)	Account Management | Privileged User Accounts					PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
*AC-2(8)	Account Management | Dynamic Account Management					PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
*AC-2(9)	Account Management | Restrictions on Use of Shared and Group Accounts					PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-2(11)	Account Management | Usage Conditions				x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-2(12)	Account Management | Account Monitoring for Atypical Usage				x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-2(13)	Account Management | Disable Accounts for High-risk Individuals			x	x	PR.AC, DE.CM, CT.DM-P, PR.AC-P	PR.AC-4, DE.CM-3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4
AC-3	Access Enforcement		x	x	x	PR.AC, PR.PT, CT.PO-P,	PR.AC-4, PR.PT-3, CT.PO-P2,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						CT.DM-P, PR.AC-P, PR.PT-P	CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(3)	Access Enforcement | Mandatory Access Control					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(4)	Access Enforcement | Discretionary Access Control					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(5)	Access Enforcement | Security-relevant Information					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(7)	Access Enforcement | Role-based Access Control					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(8)	Access Enforcement | Revocation of Access Authorizations					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(9)	Access Enforcement | Controlled Release					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							PR.AC-P4, PR.PT-P2
*AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(11)	Access Enforcement | Restrict Access to Specific Information Types					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(12)	Access Enforcement | Assert and Enforce Application Access					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(13)	Access Enforcement | Attribute-based Access Control					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
AC-3(14)	Access Enforcement | Individual Access	x				PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
*AC-3(15)	Access Enforcement | Discretionary and Mandatory Access Control					PR.AC, PR.PT, CT.PO-P, CT.DM-P, PR.AC-P, PR.PT-P	PR.AC-4, PR.PT-3, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2
AC-4	Information Flow Enforcement			x	x	ID.AM, PR.AC, PR.DS,	ID.AM-3, PR.AC-5, PR.DS-5,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(1)	Information Flow Enforcement | Object Security and Privacy Attributes					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(2)	Information Flow Enforcement | Processing Domains					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
AC-4(4)	Information Flow Enforcement | Flow Control of Encrypted Information				x	ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(5)	Information Flow Enforcement | Embedded Data Types					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(6)	Information Flow Enforcement | Metadata					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(7)	Information Flow Enforcement | One-way Flow Mechanisms					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(8)	Information Flow Enforcement | Security and Privacy Policy Filters					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(9)	Information Flow Enforcement | Human Reviews					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P,	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						PR.AC-P, PR.DS-P	PR.AC-P5, PR.DS-P5
*AC-4(10)	Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(11)	Information Flow Enforcement | Configuration of Security or Privacy Policy Filters					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(12)	Information Flow Enforcement | Data Type Identifiers					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(13)	Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(14)	Information Flow Enforcement | Security or Privacy Policy Filter Constraints					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(15)	Information Flow Enforcement | Detection of Unsanctioned Information					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(17)	Information Flow Enforcement | Domain Authentication					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(19)	Information Flow Enforcement | Validation of Metadata					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(20)	Information Flow Enforcement | Approved Solutions					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
*AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(22)	Information Flow Enforcement | Access Only					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(23)	Information Flow Enforcement | Modify Non-releasable Information					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(24)	Information Flow Enforcement | Internal Normalized Format					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(25)	Information Flow Enforcement | Data Sanitization					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(26)	Information Flow Enforcement | Audit Filtering Actions					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(27)	Information Flow Enforcement | Redundant/independent Filtering Mechanisms					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(28)	Information Flow Enforcement | Linear Filter Pipelines					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(29)	Information Flow Enforcement | Filter Orchestration Engines					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(30)	Information Flow Enforcement | Filter Mechanisms Using Multiple Processes					ID.AM, PR.AC,	ID.AM-3, PR.AC-5,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(31)	Information Flow Enforcement | Failed Content Transfer Prevention					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
*AC-4(32)	Information Flow Enforcement | Process Requirements for Information Transfer					ID.AM, PR.AC, PR.DS, DE.AE, CT.DM-P, PR.AC-P, PR.DS-P	ID.AM-3, PR.AC-5, PR.DS-5, DE.AE-1, CT.DM-P2, PR.AC-P5, PR.DS-P5
AC-5	Separation of Duties			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-6	Least Privilege			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-6(1)	Least Privilege | Authorize Access to Security Functions			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-6(2)	Least Privilege | Non-privileged Access for Nonsecurity Functions			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-6(3)	Least Privilege | Network Access to Privileged Commands				x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
*AC-6(4)	Least Privilege | Separate Processing Domains					PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-6(5)	Least Privilege | Privileged Accounts			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
*AC-6(6)	Least Privilege | Privileged Access by Non-organizational Users					PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-6(7)	Least Privilege | Review of User Privileges			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
*AC-6(8)	Least Privilege | Privilege Levels for Code Execution					PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-6(9)	Least Privilege | Log Use of Privileged Functions			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions			x	x	PR.AC, PR.DS, PR.AC-P, PR.DS-P	PR.AC-4, PR.DS-5, PR.AC-P4, PR.DS-P5
AC-7	Unsuccessful Logon Attempts		x	x	x		
*AC-7(2)	Unsuccessful Logon Attempts | Purge or Wipe Mobile Device						
*AC-7(3)	Unsuccessful Logon Attempts | Biometric Attempt Limiting						
*AC-7(4)	Unsuccessful Logon Attempts | Use of Alternate Authentication Factor						
AC-8	System Use Notification		x	x	x	CM.AW-P	CM.AW-P1
*AC-9	Previous Logon Notification						
*AC-9(1)	Previous Logon Notification | Unsuccessful Logons						
*AC-9(2)	Previous Logon Notification | Successful and Unsuccessful Logons						
*AC-9(3)	Previous Logon Notification | Notification of Account Changes						
*AC-9(4)	Previous Logon Notification | Additional Logon Information						
AC-10	Concurrent Session Control				x	PR.AC, PR.AC-P	PR.AC-5, PR.AC-P5
AC-11	Device Lock			x	x		
AC-11(1)	Device Lock | Pattern-hiding Displays			x	x		
AC-12	Session Termination			x	x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*AC-12(1)	Session Termination | User-initiated Logouts					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*AC-12(2)	Session Termination | Termination Message					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
*AC-12(3)	Session Termination | Timeout Warning Message					PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
AC-14	Permitted Actions Without Identification or Authentication		x	x	x	PR.AC, PR.AC-P	PR.AC-4, PR.AC-7, PR.AC-P4, PR.AC-P6
*AC-16	Security and Privacy Attributes					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(1)	Security and Privacy Attributes | Dynamic Attribute Association					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(2)	Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
*AC-16(3)	Security and Privacy Attributes | Maintenance of Attribute Associations by System					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(4)	Security and Privacy Attributes | Association of Attributes by Authorized Individuals					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(5)	Security and Privacy Attributes | Attribute Displays on Objects to Be Output					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(6)	Security and Privacy Attributes | Maintenance of Attribute Association					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(7)	Security and Privacy Attributes | Consistent Attribute Interpretation					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(8)	Security and Privacy Attributes | Association Techniques and Technologies					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(9)	Security and Privacy Attributes | Attribute Reassignment — Regrading Mechanisms					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
*AC-16(10)	Security and Privacy Attributes | Attribute Configuration by Authorized Individuals					PR.AC, CT.DM-P, CT.DP-P, CM.AW-P, PR.AC-P	PR.AC-4, PR.AC-6, CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6
AC-17	Remote Access		x	x	x	PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3
AC-17(1)	Remote Access | Monitoring and Control			x	x	PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption			x	x	PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3
AC-17(3)	Remote Access | Managed Access Control Points			x	x	PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3
AC-17(4)	Remote Access | Privileged Commands and Access			x	x	PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3
*AC-17(6)	Remote Access | Protection of Mechanism Information					PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3
*AC-17(9)	Remote Access | Disconnect or Disable Access					PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3
*AC-17(10)	Remote Access | Authenticate Remote Commands					PR.AC, PR.PT, PR.AC-P, PR.PT-P	PR.AC-3, PR.PT-4, PR.AC-P3, PR.PT-P3
AC-18	Wireless Access		x	x	x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
AC-18(1)	Wireless Access | Authentication and Encryption			x	x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
AC-18(3)	Wireless Access | Disable Wireless Networking			x	x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
AC-18(4)	Wireless Access | Restrict Configurations by Users				x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
AC-18(5)	Wireless Access | Antennas and Transmission Power Levels				x	PR.PT, PR.PT-P	PR.PT-4, PR.PT-P3
AC-19	Access Control for Mobile Devices		x	x	x	PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
AC-19(4)	Access Control for Mobile Devices | Restrictions for Classified Information					PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption			x	x	PR.AC, PR.AC-P	PR.AC-3, PR.AC-P3
AC-20	Use of External Systems		x	x	x	ID.AM, PR.AC, PR.AC-P	ID.AM-4, PR.AC-3, PR.AC-P3
AC-20(1)	Use of External Systems | Limits on Authorized Use			x	x	ID.AM, PR.AC, PR.AC-P	ID.AM-4, PR.AC-3, PR.AC-P3
AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use			x	x	ID.AM, PR.AC, PR.AC-P	ID.AM-4, PR.AC-3, PR.AC-P3
*AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use					ID.AM, PR.AC, PR.AC-P	ID.AM-4, PR.AC-3, PR.AC-P3
*AC-20(4)	Use of External Systems | Network Accessible Storage Devices — Prohibited Use					ID.AM, PR.AC, PR.AC-P	ID.AM-4, PR.AC-3, PR.AC-P3
*AC-20(5)	Use of External Systems | Portable Storage Devices — Prohibited Use					ID.AM, PR.AC, PR.AC-P	ID.AM-4, PR.AC-3, PR.AC-P3
AC-21	Information Sharing			x	x	PR.IP, CT.DM-P, PR.PO-P	PR.IP-8, CT.DM-P2, PR.PO-P6
*AC-21(1)	Information Sharing | Automated Decision Support					PR.IP, CT.DM-P, PR.PO-P	PR.IP-8, CT.DM-P2, PR.PO-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
*AC-21(2)	Information Sharing | Information Search and Retrieval					PR.IP, CT.DM-P, PR.PO-P	PR.IP-8, CT.DM-P2, PR.PO-P6
AC-22	Publicly Accessible Content		x	x	x		
*AC-23	Data Mining Protection					CT.DP-P	CT.DP-P1, CT.DP-P2, CT.DP-P3
*AC-24	Access Control Decisions					PR.AC, PR.AC-P	PR.AC-4, PR.AC-P4
*AC-24(1)	Access Control Decisions | Transmit Access Authorization Information					PR.AC, PR.AC-P	PR.AC-4, PR.AC-P4
*AC-24(2)	Access Control Decisions | No User or Process Identity					PR.AC, PR.AC-P	PR.AC-4, PR.AC-P4
*AC-25	Reference Monitor						

APPENDIX C: USER NOTIFICATION WARNING BANNER

Following is the standard warning banner/system-use notification that should be presented to users of internet-accessible production web applications and ED websites with the exception of Institute of Education Sciences' websites that adhere to the Education Science Reform Act.

Warning

You are accessing a U.S. Federal Government computer system intended to be solely accessed by individual users expressly authorized to access the system by the U.S. Department of Education. Usage may be monitored, recorded, and/or subject to audit. For security purposes and in order to ensure that the system remains available to all expressly authorized users, the U.S. Department of Education monitors the system to identify unauthorized users. Anyone using this system expressly consents to such monitoring and recording.

Unauthorized use of this information system is prohibited and subject to criminal and civil penalties. Except as expressly authorized by the U.S. Department of Education, unauthorized attempts to access, obtain, upload, modify, change, and/or delete information on this system are strictly prohibited and are subject to criminal prosecution under 18 U.S.C § 1030, and other applicable statutes, which may result in fines and imprisonment. For purposes of this system, unauthorized access includes, but is not limited to: Any access by an employee or agent of a commercial entity, or other third party, who is not the individual user, for purposes of commercial advantage or private financial gain (regardless of whether the commercial entity or third party is providing a service to an authorized user of the system); and Any access in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State. If system monitoring reveals information indicating possible criminal activity, such evidence may be provided to law enforcement personnel.