Information Technology (IT) Program Management (PM) Standard

January 31, 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: 2023.01.30 15:21:47 -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 IAS; address new security measures required by Executive Order (EO) 14028, and OMB regulations and memoranda and updated NIST guidance issued in response to EO 14028.
1.2	1/31/2023	Annual review. Update broken links. Add footnote to HVA control reference in Section 2.

Contents

1 INTRODUCTION

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

1.1 Purpose

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

1.2 Scope

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

2 STANDARDS

The Department standards for IT system program management controls are organized to follow

[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

the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay[5] issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

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

2.1 PM-1 Information Security Program Plan (Deployed Organization-Wide)

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

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

c. Protect the information security program plan from unauthorized disclosure and modification.

2.2 PM-2 Information Security Program Leadership Role (Deployed Organization-Wide)

Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

2.3 PM-3 Information Security and Privacy Resources (P, Deployed Organization-Wide)

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

2.4 PM-4 Plan of Action and Milestones Process (P, Deployed Organization-Wide)

a. Implement a process to ensure that plans of action and milestones (POA&M) 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.

2.5 PM-5 System Inventory (Deployed Organization-Wide and Control Overlay)

Develop and update quarterly an inventory of organizational systems.

Control Overlay PM-5 ED-01 (Organization-wide): Document and maintain the inventory of all Department technology-based information systems (i.e., the ED System Inventory) within the Department's system of record for FISMA reporting, Cyber Security Assessment and Management System (CSAM).

Control Overlay PM-5 ED-02 (Organization-wide): Register new Department technology-based

information systems by updating the ED System Inventory in CSAM upon receipt of:

a. Enterprise Architecture Technology Insertion (EATI) approval; and

b. Properly completed ED CSAM System Registration form containing all required signatures.

Control Overlay PM-5 ED-03 (Organization-wide): Determine whether a system is FISMA reportable using criteria shown in Appendix B.

Control Overlay PM-5 ED-04 (Organization-wide): Receive authorization from the EPMR prior to transferring a system or subsystem from one PO to another PO, merging a system or subsystem with another system or subsystem.

Control Overlay PM-5 ED-05 (Organization-wide): Document system and subsystem transfers or mergers using the current version of the Department authorized Memorandum for the Record (MFR) template. Update the ED System Inventory within CSAM by submitting the completed MFR form along with evidence of EATI approval to the ED CSAM Support Team.

Control Overlay PM-5 ED-06 (Organization-wide): Complete the current version of the Disposal Plan and Disposal checklist and request EATI authorization prior to the disposal, decommissioning, or retirement of existing system(s) or subsystem(s) with the ED System Inventory; address actions required for all underlying systems and/or subsystems.

Control Overlay PM-5 ED-07 (Organization-wide): Update the ED System Inventory within CSAM following the authorized disposal, decommissioning or retirement of existing system(s) or subsystem(s) by changing the operational status.

2.5.1 PM-5(1) System Inventory | Inventory of Personally Identifiable Information (P, Deployed Organization-Wide)

Establish, maintain, and update quarterly an inventory of all systems, applications, and projects that process personally identifiable information.

2.6 PM-6 Measures of Performance (P, Deployed Organization-Wide)

Develop, monitor, and report on the results of information security and privacy measures of performance.

2.7 PM-7 Enterprise Architecture (P, Deployed Organization-Wide)

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.

2.7.1 PM-7(1) Enterprise Architecture | Offloading (Deployed Organization-Wide)

Offload non-essential functions or services, as feasible, to other systems, system components, or an external provider.

2.8 PM-8 Critical Infrastructure Plan (P, Deployed Organization-Wide)

Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

2.9 PM-9 Risk Management Strategy (P, Deployed Organization-Wide)

a. Develop 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.

2.10 PM-10 Authorization Process (P, Deployed Organization-Wide)

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.

2.11 PM-11 Mission and Business Process Definition (P, Deployed Organization-Wide)

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).

2.12 PM-12 Insider Threat Program (Deployed Organization-Wide)

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

2.13 PM-13 Security and Privacy Workforce (P, Deployed Organization-Wide)

Establish a security and privacy workforce development and improvement program.

2.14 PM-14 Testing, Training, and Monitoring (P, Deployed Organization-Wide)

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.

2.15 PM-15 Security and Privacy Groups and Associations (Deployed Organization-Wide)

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.

2.16 PM-16 Threat Awareness Program (Deployed Organization-Wide)

Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

2.16.1 PM-16(1) Threat Awareness Program | Automated Means for Sharing Threat Intelligence (Deployed Organization-Wide)

Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

2.17 PM-17 Protecting Controlled Unclassified Information on External Systems (P, Deployed Organization-Wide)

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).

2.18 PM-18 Privacy Program Plan (P, Deployed Organization-Wide)

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.

2.19 PM-19 Privacy Program Leadership Role (P, Deployed Organization-Wide)

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.

2.20 PM-20 Dissemination of Privacy Program Information (P, Deployed Organization-Wide)

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.

2.20.1 PM-20(1) Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services (P, Deployed Organization-Wide)

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.

2.21 PM-21 Accounting of Disclosures (P, Deployed Organization-Wide)

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.

2.22 PM-22 Personally Identifiable Information Quality Management (P, Deployed Organization-Wide)

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.

2.23 PM-23 Data Governance Body (Deployed Organization-Wide)

Establish a Data Governance Body consisting of roles defined in the ED Data Governance Board (DGB) Charter, led by the Chief Data Officer (CDO) with responsibilities as defined in the ED DGB Charter.

2.24 PM-24 Data Integrity Board (P, Deployed Organization-Wide)

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.

2.25 PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research (P, Deployed Organization-Wide)

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).

2.26 PM-26 Complaint Management (P, Deployed Organization-Wide)

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.

2.27 PM-27 Privacy Reporting (P, Deployed Organization-Wide)

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.

2.28 PM-28 Risk Framing (P, Deployed Organization-Wide)

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 the CIO, CISO, CPO/SAOP, and mission/business owners; and

c. Review and update risk framing considerations annually (i.e., each fiscal year).

2.29 PM-29 Risk Management Program Leadership Roles (Deployed Organization-Wide)

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.

2.30 PM-30 Supply Chain Risk Management Strategy (Deployed Organization-Wide)

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 annually (i.e., each fiscal year) or as required, to address organizational changes.

2.30.1 PM-30(1) Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items (Deployed Organization-Wide)

Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

2.31 PM-31 Continuous Monitoring Strategy (P, Deployed Organization-Wide)

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.

2.32 PM-32 Purposing (Deployed Organization-Wide)

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.

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

Acronym	Description
ACS	Administrative Communications System
CDO	Chief Data Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management tool
CSF	Cyber Security Framework
DGB	Data Governance Board
ED	Department of Education
EO	Executive Order
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
HVA	High Value Asset
IAS	Information Assurance Services
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PM	Program Management
POA&M	Plan of Action & Milestones
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy
SP	Special Publication

APPENDIX B: BASELINE CONTROL PARAMETER SUMMARY

The Program Management controls are implemented at the organization level and are not directed at individual information systems. The Program Management controls are designed to facilitate compliance with applicable federal laws, executive orders, directives, regulations, policies, and standards.

Table 3: Baseline Control Parameter Summary

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
PM-1	Information Security Program Plan		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.GV, DE.DP	ID.GV-2, DE.DP-2
PM-2	Information Security Program Leadership Role		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.AM, ID.GV, GV.PO-P	ID.AM-6, ID.GV-2, GV.PO-P3
PM-3	Information Security and Privacy Resources	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.GV, GV.PO-P	ID.GV-4, GV.PO-P2, GV.PO-P3, GV.PO-P6
PM-4	Plan of Action and Milestones Process	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.RA, RS.AN, ID.RA-P, GV.MT-P	ID.RA-1, ID.RA-6, RS.AN-5, ID.RA-P5, GV.MT-P4
PM-5	System Inventory		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.AM, ID.IM-P, ID.RA-P, GV.MT-P	ID.AM-1, ID.AM-4, ID.IM-P1, ID.IM-P6, ID.RA-P1, GV.MT-P1
PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.AM, ID.IM-P, ID.RA-P, GV.MT-P	ID.AM-1, ID.AM-4, ID.IM-P1, ID.IM-P6, ID.RA-P1, GV.MT-P1
PM-6	Measures of Performance	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	PR.IP, PR.PO-P	PR.IP-7, PR.PO-P5
PM-7	Enterprise Architecture	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.GV, GV.PO-P, CT.DP-P	ID.GV-4, GV.PO-P6, CT.DP-P1, CT.DP-P3
PM-7(1)	Enterprise Architecture | Offloading		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.GV, GV.PO-P, CT.DP-P	ID.GV-4, GV.PO-P6, CT.DP-P1, CT.DP-P3
PM-8	Critical Infrastructure Plan	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.BE, ID.RM	ID.BE-2, ID.BE-4, ID.RM-3
PM-9	Risk Management Strategy	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.GV, ID.RA, ID.RM, ID.SC, ID.RA-P,	ID.GV-4, ID.RA-4, ID.RA-6, ID.RM-1, ID.RM-2,

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
						ID.DE-P, GV.PO-P, GV.RM-P	ID.RM-3, ID.SC-2, ID.RA-P5, ID.DE-P2, GV.PO-P6, GV.RM-P1, GV.RM-P2
PM-10	Authorization Process	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.GV, GV.PO-P	ID.GV-4, GV.PO-P6
PM-11	Mission and Business Process Definition	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.BE, ID.GV, ID.RA, ID.RM, ID.BE-P, GV.PO-P	ID.BE-3, ID.GV-4, ID.RA-4, ID.RM-3, ID.BE-P2, GV.PO-P6
PM-12	Insider Threat Program		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.RA	ID.RA-3
PM-13	Security and Privacy Workforce	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	PR.AT, GV.PO-P, GV.AT-P	PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5, GV.PO-P3, GV.AT-P1, GV.AT-P2, GV.AT-P3
PM-14	Testing, Training, and Monitoring	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	PR.AT, PR.IP, DE.DP, GV.AT-P, GV.MT-P, PR.PO-P	PR.AT-1, PR.IP-10, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-5, GV.AT-P1, GV.MT-P3, PR.PO-P8
PM-15	Security and Privacy Groups and Associations		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.RA, RS.CO, RS.AN, GV.MT-P, CM.AW-P	ID.RA-1, ID.RA-2, RS.CO-5, RS.AN-5, GV.MT-P5, CM.AW-P2
PM-16	Threat Awareness Program		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.RA	ID.RA-2, ID.RA-3, ID.RA-5
PM-16(1)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.RA	ID.RA-2, ID.RA-3, ID.RA-5
PM-17	Protecting Controlled Unclassified Information on External Systems	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide		
PM-18	Privacy Program Plan	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.PO-P	GV.PO-P3, GV.PO-P4, GV.PO-P6
PM-19	Privacy Program Leadership Role	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.PO-P	GV.PO-P3, GV.PO-P4, GV.PO-P6
PM-20	Dissemination of Privacy Program	x	N/A -	N/A -	N/A -	GV.MT-P,	GV.MT-P7,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
	Information		Deployed organization-wide	Deployed organization-wide	Deployed organization-wide	CM.PO-P, CM.AW-P	CM.PO-P1, CM.AW-P1, CM.AW-P2
PM-20(1)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.MT-P, CM.PO-P, CM.AW-P	GV.MT-P7, CM.PO-P1, CM.AW-P1, CM.AW-P2
PM-21	Accounting of Disclosures	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	CM.AW-P	CM.AW-P4, CM.AW-P6
PM-22	Personally Identifiable Information Quality Management	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.MT-P, CT.PO-P, CM.AW-P	GV.MT-P7, CT.PO-P2, CT.PO-P3, CM.AW-P5
PM-23	Data Governance Body		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.PO-P, CT.PO-P	GV.PO-P2, GV.PO-P6, CT.PO-P2
PM-24	Data Integrity Board	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide		
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide		
PM-26	Complaint Management	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.MT-P, CM.AW-P	GV.MT-P7, CM.AW-P2
PM-27	Privacy Reporting	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.MT-P, CM.PO-P	GV.MT-P4, CM.PO-P1
PM-28	Risk Framing	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.GV, ID.RA, ID.RM, ID.RA-P, GV.PO-P, GV.RM-P	ID.GV-4, ID.RA-5, ID.RA-6, ID.RM-1, ID.RA-P4, ID.RA-P5, GV.PO-P6, GV.RM-P1, GV.RM-P3
PM-29	Risk Management Program Leadership Roles		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.AM, ID.GV, GV.PO-P	ID.AM-6, ID.GV-2, GV.PO-P3, GV.PO-P4
PM-30	Supply Chain Risk Management Strategy		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.SC, ID.DE-P	ID.SC-1, ID.DE-P1
PM-30(1)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	ID.SC, ID.DE-P	ID.SC-1, ID.DE-P1
PM-31	Continuous Monitoring Strategy	x	N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide	GV.MT-P	GV.MT-P3
PM-32	Purposing		N/A - Deployed organization-wide	N/A - Deployed organization-wide	N/A - Deployed organization-wide		

APPENDIX C: SYSTEM TYPES

Only FISMA reportable systems are required to obtain and retain an ED Authorization to Operate (ATO). Use the system types shown in Table 4 along with the guidance shown below to used determine whether a system is FISMA reportable. Note: only one type may be assigned to a system.

- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, provides guidelines for federal information systems, which have been determined as discrete sets of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether such information is in digital or non-digital form. Information resources include information and related resources, such as personnel, equipment, funds, and information technology.
- Additionally, with authorization boundaries and external providers, FISMA and OMB policy require external providers that process, store, or transmit federal information or operate information systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Federal security and privacy requirements also apply to external systems storing, processing, or transmitting federal information and any services provided by or associated with the external system.
- Lastly, this guidance outlines that an information system used or operated by an executive agency, by a contractor of an executive agency, or, by another organization on behalf of an executive agency as FISMA Reportable. Therefore, if an Information System within CSAM meets these criteria, the 'FISMA Reportable' field under System Identification should be selected accordingly.

Table 4: ED System Types

System Type	Description	FISMA Reportable
System (SYS)	A System (SYS) is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A SYS requires special management oversight because of its importance to the mission of the Department or a PO; its high development, operating, or maintenance costs; or its significant role in the administration of Department or PO programs, finances, property, or other resources. A SYS may include many individual programs and hardware, software, and telecommunications components. These components can be a single software application, or a combination of hardware/software focused on supporting a specific, mission-related function. A SYS may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or	Yes

	personnel). SYS require a Department specific ATO. A SYS inherits controls from the ED Program and may inherit controls from other programs, systems and subsystems. A SYS may also serve as a Common Control Provider (CCP) and offer controls for inheritance to other systems and subsystems. A SYS may serve as a parent system to one or more subsystems (e.g., child systems) which are included in its authorization boundary, documented in its system security plan (SSP) and supporting appendices, and covered by its ATO memorandum. Previously SYS were identified as General Support Systems (GSS) and Major Applications (MAJ). Cloud Service Providers (CSP) providing Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are SYS. Cloud dependent systems are typically SYS as these systems are not included in the CSP's SSP and authorization boundary.	
Subsystem (SUB)	A Subsystem (SUB) is a major subdivision of an SYS consisting of information, information technology, personnel, etc. that perform one or more specific functions. A SUB must be designated as a child of a parent system and must be included in the parent system's authorization boundary, SSP and supporting appendices, and ATO memorandum. As SUBs are authorized through the parent system's ATO, no separate ATO for the SUB is required. A SUB must be assigned a security category in accordance with FIPS 199 which is equal to or less than that assigned to its parent system. SUBs must document system specific information and controls within CSAM. A SUB inherits controls from the ED Program, its parent system, and may inherit controls from other SUBs within its parent system's authorization boundary. In certain situations, a SUB may serve as a CCP and offer controls for inheritance to its parent system and other SUBs within its parent system's authorization boundary. Previously many SUBs may have been labeled as Minor (MIN) applications.	No
Federal Shared Service	A Federal shared service is a business or mission function that is provided for consumption by multiple organizations within or between Federal agencies. Shared services enable the Department of Education to efficiently aggregate resources and systems to improve the quality, timeliness, and cost effectiveness of service delivery. The external agency which owns the service is responsible for authorizing the information to operate and the Department is responsible for explicitly accepting the risk to use the service based	No

	on agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of controls in the system or service. All Federal shared services shall be registered in the Department's official FISMA system inventory within CSAM. Federal Shared Services are managed via an Inter-Agency Agreement (IAA) and no explicit ED ATO is required based on the information in an existing authorization package generated by the providing agency. However, information necessary to manage the ED use of the shared service must be documented within CSAM. This includes the shared service's hosting location, FIPS categorization, information types, Information System Owner (ISO), Information System Security Officer (ISSO), Authorizing Official (AO), and Risk Executive. The SSP must also be signed by the designated ISO and ISSO.	
Program	Each PO is represented within CSAM using a program. Programs are used to document and track PO Business Continuity Plans (BCP), document PO specific controls and offer those controls for inheritance to SYS and SUBs within the PO, and document and track Plans of Action and Milestones (POA&Ms) assigned to the PO.	No