ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL HANDBOOK

Distribution:
All Department of Education Employees

Approved by: _____/s_____
Andrew Jackson
Assistant Secretary for Management

Information Assurance/Cybersecurity Policy

Table of Contents

1. INTRODUCTION 4
1.1 Purpose 4
1.2 Scope 4
1.3 Authority 4
1.4 Applicability 5
1.5 Exceptions 5
1.6 Governance Framework 5
1.6.1 Level 1: Enterprise 6
1.6.2 Level 2: System 7
1.6.3 Level 3: Application 7
2. ROLES AND RESPONSIBILITIES 7
2.1 Secretary 8
2.2 Deputy Secretary 8
2.3 Office of the General Counsel 8
2.4 Office of Inspector General 8
2.5 Office of Management 9
2.5.1 Chief Privacy Officer 9
2.5.2 Senior Privacy Specialist 9

2.6 Office of the Chief Information Officer 10
2.6.1 Chief Information Officer 10
2.6.2 Chief Information Security Officer 11
2.6.3 Department Information System Security Manager (ED ISSM) 12
2.6.4 Department Computer Incident Response Capability (EDCIRC) 13
2.6.5 Department Security Operations Center (EDSOC) 13
2.7 Principal Offices 13
2.7.1 Director, Information Assurance Services 13
2.7.2 Principal Officer 14
2.7.3 Authorizing Officials 15
2.7.4 Information System Owner 15
2.7.5 Information System Security Officers 16
2.8 Users 17
3. POLICY RESPONSIBILITIES, ORGANIZATIONS, AND DOCUMENTS 17
3.1 FISMA, FIPS-199, and OMB Circular A-130 17
3.2 FISMA Reporting 18
3.3 Capital Planning and Investment Control 18
3.4 Security Authorization 18
3.5 Risk Assessment and Management 19
3.6 Critical Infrastructure Protection (CIP) 19
3.7 Protection of National Security Information 19
3.8 Records Management 20
3.9 Lifecycle Management 20
3.10 FIPS-200 and NIST Special Publication 800-53 20
3.11 Access Control 21
3.12 Identification and Authentication 21
3.13 Physical and Environmental Security 21
3.14 Personnel Security 21
3.15 Continuity of Operations, Disaster Recovery, and Contingency Plans 22
3.16 Internet Use and Controls 22
3.17 The Privacy Act, Privacy Assessments, and System of Records Notices 23
3.18 Remote Access and Telework 24
3.19 Interconnection Security and Computer Matching Agreements 24
3.20 Cloud Computing 25
3.21 Configuration Management 25
3.22 Incident Response 26
3.23 Awareness and Training 26
3.24 Wireless and Mobile Device Security 27
APPENDIX A: DEFINITIONS 28
APPENDIX B: ACRONYMS 30
APPENDIX C: REFERENCES 31

Document Configuration Control

Version	Release Date	Summary of Changes	Affected Page Number(s)
1.0	08/01/04	Document Developed	All
2.0	03/01/05	Administrative Communications System (ACS) Review changes	
3.0	06/01/05	ACS Final Document	
4.0	08/01/05	ACS Release	
5.0	10/19/11	ACS Release	
5.1	03/16/12	Comments received via ACS and incorporated	All
6.0	10/20/11	ACS Release	
6.1	05/28/13	ACS review and major update, including numbering change	All
6.2	06/08/13	Minor updates	All
6.3	07/15/13	Minor updates	All
6.4	08/19/13	Minor Updates	All
6.5	10/29/13	Major updates to section 3, minor updates to sections 1 & 2	All
6.6	12/03/13	Minor corrections/updates due to comments submitted	All
6.7	02/18/14	Minor corrections/updates due to comments submitted	All

1. INTRODUCTION

Cybersecurity is a critical area for all organizations as attacks against information and information systems continue to increase and become more complex. To protect against these attacks requires a solid foundation of information assurance (IA) and cybersecurity measures to manage the risks related to the use, processing, storage and transmission of information and the systems and processes used for those purposes.

1.1 Purpose

The purpose of this *Information Assurance (IA)/Cybersecurity Policy* (Policy) is to provide policy from the Office of the Chief Information Officer (OCIO) regarding IA/cybersecurity for all Information Technology (IT) assets and services operated within or on behalf of the U.S. Department of Education (the Department).

This IA/Cybersecurity Policy is supported through standards, guidance, directives, and other IAS governance documents and shall be complied with in full.

1.2 Scope

This Policy addresses IA/cybersecurity. Additional policies addressing personnel, privacy, and physical security have been issued separately by the departmental offices responsible for those programs. However, those aspects of personnel, privacy, and physical security that relate to IA/cybersecurity are covered in this Policy. In the event of inconsistency on matters relating to personnel, privacy, and physical security, this Policy shall control. Employees with IA/cybersecurity responsibilities shall coordinate with Department officials (e.g., facilities managers, personnel managers, and privacy officials) to implement an effective information security program.

1.3 Authority

This Policy is based on statutory and executive directive requirements that include Federal laws and regulations, Presidential Directives and Executive Orders, National Institute of Standards and Technology (NIST) Special Publications (SP) 800 Series, NIST Federal Information Processing Standards (FIPS), Office of Management and Budget (OMB) Circulars, and Department of Homeland Security (DHS) policy. Refer to Appendix C for a more complete list of applicable governance.

Violation of this Policy may result in loss of, or limitations on, use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution in accordance with Federal law and Department policy.

1.4 Applicability

This Policy applies to all Department personnel and contractor support staff. Additionally, it applies to all Department IT resources; hardware; software; media; facilities; and data owned, managed, or operated on behalf of the Department. Compliance with this Policy is mandatory; exceptions to the Policy must be approved in accordance with the processes described herein.

This Policy identifies roles and assigns responsibilities in support of the Department's IA/cybersecurity mission. To support the success of the Department's IA/cybersecurity mission, all personnel and support contractors must be familiar with, and comply with, policy contained in this document.

1.5 Exceptions

All requirements in this Policy may not be achievable. In these circumstances, the Principal Office must assess the risk and make a risk-based decision not to meet the requirements based on one or more of the following criteria:

- The implementation of the requirement would impose greater overall risk on the system than would the exception
- Alternative controls (technical or procedural) have been implemented that will reduce the risk to levels at or below what the requirement would have provided
- The cost of implementing the requirement is not commensurate with the reduction in risk that is offered by the requirement
- The implementation of the requirement is technically infeasible or will disrupt or severely degrade system functionality.

Documentation of the risk decision must accompany the request and show what steps have been taken to ensure that the risk is reduced to an acceptable level, identifying the exception, the operational risk acceptance, and the risk mitigation measures. The Principal Office's Authorizing Official (AO) must submit the risk decision through the Department's Chief Information Security Officer (CISO). The CISO will review the risk decision and forward it to the Chief Information Officer (CIO) for approval.

1.6 Governance Framework

IA Governance is the structure through which information assurance is achieved to ensure that information and information system risks are managed appropriately. The governance framework is the term used to describe the group of Information Assurance Services (IAS) policies, standards, guidance, standard operating procedures (SOPs), and other related documents that define the

methods to protect against unauthorized access or attacks. The IAS Governance Framework is based on three levels (Enterprise, System and Application) and the following attributes:

- Originating Authority – The authority that develops and owns the governance documents
- Approval Process Owner– The Group/Organization who owns the approval process for governance types
- Document Approver – The final/highest authority signer of the governance document
- Content Ownership – The individual/Subject Matter Expert (SME)/group who is responsible for creating/updating the content, not necessarily the Document Owner
- Document Ownership – The individual/SME/group responsible for ensuring the content in the document is kept up-to-date, this can be different from the Content Owner
- Key Stakeholders – The individuals who are directly affected by the governance document and will review draft documents to provide comments

1.6.1 Level 1: Enterprise

The Level 1 governance documents are the highest-level documents in the Department. They include policies and directives that affect all employees and support staff.

Level 1: Enterprise (policies/directives)

- Originating Authority: Federal laws, Executive Orders/Directives, Mandated Standards (NIST), Best Practices, and/or Department policy
- Approval Process Owner: OM ACS
- Document Approver: ED CIO & CISO (through ACS process)
- Content Ownership: CISO/IAS Branch Chiefs/FSA Security Team
- Document Ownership: Policy & Planning Branch
- Key Stakeholders: All Principal Offices (POs), OGC, OIG, Union.

1.6.2 Level 2: System

The Level 2 governance documents are middle tier documents which include standards, guidance, and directive memoranda. These documents mainly affect Department systems and networks.

Level 2: System (standards/guidance/memos)

- Originating Authority: Federal laws, Executive Orders/Directives, Mandated Standards (NIST), Best Practices, Department & OCIO policy (Level 1)
- Approval Process Owner: IAS
- Document Approver: ED CISO
- Content Ownership: CISO/IAS Branch Chiefs
- Document Ownership: Policy & Planning Branch
- Key Stakeholders: POs, ISSOs, System Owners, SMEs.

1.6.3 Level 3: Application

The Level 3 governance documents are the lowest tier of documents and include procedures and processes. These documents affect individual systems and applications.

Level 3: Application (processes/procedures/templates)

- Originating Authority: IAS standards (Level 2)
- Approval Process Owner: IAS
- Document Approver: ED IAS Branch Chiefs
- Content Ownership: IAS Branch Chiefs/SMEs
- Document Ownership: IAS Branch Chiefs
- Key Stakeholders: POs, ISSOs, System Owners

2. ROLES AND RESPONSIBILITIES

The roles and responsibilities described in this chapter ensure effective implementation and management of the Department's IA/cybersecurity mission. OMB Circular A-130, *Management of Federal Information Resources* requires

the establishment of a security management structure and assignment of security responsibilities. Unless otherwise noted, all personnel fulfilling the requirements of the identified roles must be appropriately cleared United States Government employees.

2.1 Secretary

The Secretary is responsible for the overall IA/cybersecurity mission and funding within the Department. The Secretary provides the oversight for developing and implementing the IT security policies, principles, standards, and guidelines that form the basis of a comprehensive IA/cybersecurity program.

2.2 Deputy Secretary

Acting on behalf of the Secretary, the Deputy Secretary oversees the OCIO development and execution of IA/cybersecurity policies, standards, procedures, and guidelines for handling the Department's information and IT resources to improve the efficiency, effectiveness, and security of operations.

2.3 Office of the General Counsel

The Office of the General Counsel (OGC) is responsible for providing counsel and legal advice to the Secretary, Directors, and Department employees, in developing and implementing IA/cybersecurity policies, principles, standards, and guidelines that form the basis of a comprehensive IA/cybersecurity program.

2.4 Office of Inspector General

The Office of Inspector General (OIG) is charged with promoting the efficiency, effectiveness, and integrity of the Department's IA/cybersecurity programs and operations. The OIG conducts independent and objective audits, investigations, inspections, and other activities to evaluate Department's security program compliance with established Federal mandates, laws, and directives, and to assess the effectiveness of its operation.

The OIG is the Department's principal law enforcement component responsible for the investigation of potential criminal and civil violations of Federal law, as they relate to Department's programs and operations. This includes, but is not limited to, any matter involving denial of service, unauthorized access, exceeding authorized access, criminal misuse (e.g., child pornography) of IT resources as well as the illegal interception of electronic communications. The OIG is the only departmental component authorized to make referrals to the Department of Justice or the Federal Bureau of Investigation (FBI) respecting criminal matters.

In addition, under the Federal Information Security Management Act of 2002 (FISMA), the OIG participates in providing a comprehensive annual review of Department's IA/cybersecurity program. The OIG reports on the adequacy and

effectiveness of information security policies, procedures, and practices in plans and reports relating to annual Department budgets, information resources management, results-based management, program performance, and financial management.

2.5 Office of Management

The Office of Management (OM) leads the effort to transform the Department into a high-performance, customer-focused organization by providing services to their customers that help them do a better job of managing their people, processes, technology, and overall strategy.

2.5.1 Chief Privacy Officer

The Chief Privacy Officer (CPO) is the senior Departmental official with the overall Department-wide responsibility for information privacy issues. The CPO is also accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems. The CPO has the following responsibilities:

- Reviewing and approving all Privacy Impact Assessments (PIA) and System of Records Notices (SORNs) to ensure that they meet the requirements of Section 208 of the *E-Government Act of 2002*, and of the *Privacy Act of 1974*, as amended, respectively

- Implementing the Department's privacy program, including coordinating policy development, providing outreach and training, and working with the OCIO to integrate safeguards for data protection and system security

2.5.2 Senior Privacy Specialist

The Senior Privacy Specialist, designated by the Chief Privacy Officer, is responsible for managing the Department's Privacy Act Program. The Senior Privacy Specialist administers activities related to the establishment, alteration, or termination of SORNs and PIAs. The Senior Privacy Specialist, or designee, has the following responsibilities:

- Providing guidance and technical assistance to individuals who are developing the documentation required for PIAs and SORNs

- Working with the Department's Computer Incident Response Capability (EDCIRC) Coordinator on all security breaches that involve PII.

Privacy duties are described in more detail in OM: 6-104, *The Collection, Use, and Protection of Personally Identifiable Information and of Records Maintained in Privacy Act Systems of Records*.

2.6 Office of the Chief Information Officer

OCIO provides the technological solutions that enable the Department to deliver services to schools, students and their families. OCIO advises and assists the Secretary and other senior officers in acquiring IT and managing information resources. OCIO helps these leaders comply with the best practices in the industry and applicable federal laws and regulations.

2.6.1 Chief Information Officer

As the Senior Department official responsible for information resources management, the Chief Information Officer (CIO) develops, oversees and manages the Department's IA/cybersecurity mission. Additionally, the CIO provides advice and other assistance to the Secretary, Deputy Secretary and other senior officers on IT matters. The CIO's significant security-related duties include:

- Designating a Chief Information Security Officer (CISO) to execute the Department's IA/cybersecurity mission
- Overseeing the development and maintenance of IA/cybersecurity policy, procedures, and control techniques to address all applicable requirements
- Ensuring security considerations are integrated into the Department IT architecture, planning and budgeting cycles, and system development lifecycle
- Developing IA/cybersecurity requirements to fulfill the IA/cybersecurity responsibilities authorized by Federal law, government-wide regulations, and mandates
- Providing oversight, guidance, and support to Department IA/cybersecurity personnel
- Complying with Federal IA/cybersecurity mandates
- Providing senior management input and oversight for IA/cybersecurity risk management-related activities across the organization
- Developing and maintaining reliable IA/cybersecurity cost estimates to secure adequate funding, resources, and training for the IA/cybersecurity mission

- Coordinating reports to the OMB, the DHS and others as required about the overall effectiveness of Department's IA/cybersecurity mission, including progress of remedial actions

2.6.2 Chief Information Security Officer

The Chief Information Security Officer (CISO) is responsible for the development, implementation, effectiveness, and oversight of the Department's IA/cybersecurity program, in accordance with the IA/cybersecurity mission. The CISO's responsibilities include:

- Executing the CIO's responsibilities with respect to FISMA, FIPSs, OMB Circulars A-11*, Preparation, Submission, and Execution of the Budget*, A-123, *Management's Responsibility for Internal Control* and A-130, *Management of Federal Information Resources*

- Serving as the CIO's primary liaison to Departmental Authorizing Officials

- Ensuring authorization decisions consider all factors necessary for Department mission and business success

- Coordinating enterprise IA/cybersecurity risk management activities, including setting risk thresholds, to maintain consistent risk acceptance decisions for Department IT assets, services, operations, and individuals

- Advising the CIO of any risks regarding IT vulnerabilities or issues that may have an adverse impact on the Department

- Appointing the Department's Information System Security Manager (ISSM)

- Appointing and supervising an Education Computer Incident Response Capability (EDCIRC) Coordinator.

- Establishing and maintaining a Department Configuration Management Plan that includes an accurate, complete, and up-to-date system inventory and addresses, for each system, all phases of system life, including development/procurement, installation, operation, maintenance and patch management, and system disposal

- Ensuring that a FISMA performance metrics program is developed, implemented, and funded

- Coordinating Department-wide IT security incident reporting and emergency response activities, and serving as the Department liaison with the OGC, United States Computer Emergency Response Team (US-CERT), the FBI,

OIG, and other external law enforcement agencies concerning IT security incident reporting and follow-up activities

- Establishing and maintaining a cybersecurity operations capability to actively monitor and respond to cyber incidents.
- Participating in Department Statement of Work (SOW) reviews to include appropriate IA/cybersecurity language in contracts for IT services
- Creating, maintaining and disseminating the Department's documented IA/cybersecurity posture.
- Establishing and overseeing a Department Vulnerability Management Plan and associated policy(s) and procedures to ensure that the Department maintains secure configuration of all Department systems and assets.

The CISO, or an appointed delegate, will review this policy at least annually to:

- Reflect any changes in Federal laws and regulations
- Satisfy additional business requirements
- Encompass new technology
- Adopt new Federal government IT standards.

2.6.3 Department Information System Security Manager (ED ISSM)

The Department's ISSM supports the CISO in the execution of the Department's IA/cybersecurity program. ED ISSM serves as the liaison and primary point of contact and coordination between PO personnel responsible for IA/cybersecurity activities and the CISO for IT security matters. ED ISSM's responsibilities include:

- Advising the CISO, AOs, ISOs, and ISSOs, on information security risks associated with current and planned information systems
- Managing the Department's Security Authorization Program
- Ensuring, through coordination with the EDCIRC and the Department's Computer Security Operations Center (EDSOC), that all departmental systems are in compliance with IA/cybersecurity policy and reporting the status to the CISO, applicable PO AO and ISSO
- Serving as a member of, and representing IA/cybersecurity interests to, the Enterprise Architecture Review Board (EARB)

- Providing input to security awareness and related training programs and distributing security awareness information to the ISSO community as appropriate

- Remaining current on duties pertinent to roles and responsibilities of an ISSM.

2.6.4 Department Computer Incident Response Capability (EDCIRC)

The primary mission of the EDCIRC is to serve as the focal point for Information Security Incident Management for the Department. The EDCIRC's objective is to provide the ability to rapidly report and respond to incidents and resolve them with minimal impact to the Department. The EDCIRC also assists in the prevention of incidents by engaging in trend analysis and mitigation planning. The EDCIRC consists of matrixed personnel from various organizations within the Department and is organized under the EDCIRC Coordinator.

2.6.5 Department Security Operations Center (EDSOC)

The primary mission of the EDSOC is to provide the continuous and independent monitoring and defense of the Department's information infrastructure and assets ensuring the protection and availability of the information entrusted to the Department. The EDSOC's primary objectives are to provide 24 X 7 X 365 surveillance, situational monitoring, and cyber defense services; to provide the ability to rapidly detect and identify malicious activity and to promptly subvert that activity by lawful means; and to collect data and maintain metrics that demonstrate the impact of the Department's cyber defense approach, its cyber state and cyber security posture.

2.7 Principal Offices

2.7.1 Director, Information Assurance Services

The Director, Information Assurance Services (IAS) is responsible for the development, implementation, effectiveness, and oversight of the Department's IA/cybersecurity mission. The Director, IAS, serves as the central repository for all Department IT system security documents, including Security Authorization documentation. The Director may require changes to any such documents to ensure their completeness, consistency, and adequacy in meeting and conforming to Department IA/cybersecurity standards and policies. The Director's responsibilities include:

- Serving as the CIO's principal point of contact for matters relating to the security of the Department's systems and IT resources

- Maintaining the Department's list of General Support Systems and Major Applications

- Monitoring, evaluating, and reporting annually to the CIO on the status and adequacy of the IA security policy and program within the Department

- Monitoring corrective actions resulting from IT security assessments, surveys, and audits.

2.7.2 Principal Officer

The Principal Officer is the senior individual administratively and operationally responsible for all computer systems within the PO or major component. The Principal Officer may rely upon an information system in the fulfillment of a business function. The Principal Officer has centralized responsibility for the establishment, maintenance, and enforcement of the IA/cybersecurity program and policy for all IT supporting systems within the Principal Office or business component. Specific security-related responsibilities of the Principal Officer include, but are not limited to:

- Ensuring the duties of the AO for Security Authorization activities are completed

- Maintaining an up-to-date listing of the systems under his/her control within the PO

- Applying management, operational, and technical security controls, as appropriate, that are commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information for all systems under his/her control or subject to his/her use

- Managing personnel, information, and physical security matters within the PO

- Ensuring that a security self-assessment is completed for each system at least annually that is consistent with the Security Authorization requirements and notify the Department's CIO of any changes

- Ensuring that all PO systems are authorized for operation in accordance with the Department's Security Authorization Program

- Ensuring, in coordination with the Director, IAS, and contracting officers, that IA/cybersecurity is addressed in all IT-related procurements and contracts

- Ensuring current system inventories, system-level security plans, security reviews, corrective action plans, Security Authorization packages, and similar

IA/cybersecurity documents are developed and maintained and forwarded to the Director, IAS.

2.7.3 Authorizing Officials

An Authorizing Official (AO) is a senior official of a PO who is accountable for the security risks associated with an information system and possesses a sufficient level of authority to accept system-related security risks. The Principal Officer shall assign an AO for each PO system. The role of AO has inherent U.S. Government authority, and should be assigned to government personnel only, typically with budgetary oversight or responsibility for the mission or business operations supported by the system(s). The AO cannot be an information system owner/manager. The AO is responsible for ensuring the system operates at a risk level acceptable to the Department. AO responsibilities include:

- Ongoing authorizing a system to operate and denying that authorization if security risks identified are deemed unacceptable
- Approving security requirements, security plans/reports, and plans of action and milestones (POA&M) and determining if any change in the system requires reauthorization to operate
- Ensuring proper agreements are in place with internal and external entities when systems share services or data
- Participating in IA/cybersecurity risk management activities including maintaining consistent risk acceptance decisions and consulting with other AOs and Department officials to inform them of, and justify, any residual risks
- Ensuring that all activities and functions associated with security authorization, which may be delegated to an officially designated representative(s), are completed
- Budgeting IA/cybersecurity costs for IT systems and services for the PO
- Assigning an ISO and ISSO for each PO system.

2.7.4 Information System Owner

The Information System Owner (ISO) is assigned by the Authorizing Official (AO) and has the responsibility for the development, operation and continuous monitoring of the system(s). ISOs also ensure that the operational interests of their user community are addressed.

Specific to security, ISOs are responsible for the development and maintenance of the System Security Plan (SSP) and ensuring that all appropriate officials are informed of security concerns necessary to properly continually authorize the

system for operation. Specifically, if any security weaknesses are identified during the development or operation of the system, the ISO is responsible for developing a Plan of Actions and Milestones (POA&M) to document and mitigate the weaknesses. The POA&M shall address:

- All security weaknesses that have been identified as part of the Authorization process
- The corrective actions that have been taken or are planned to mitigate the weakness, along with the milestones and dates that indicate to management that these corrective measures have been taken
- Security weaknesses that have not been mitigated, and for which the associated residual risk has been agreed to and accepted by the AO.

2.7.5 Information System Security Officers

The AO formally designates the Information System Security Officer (ISSO) to be responsible for the implementation and management of the departmental IA/cybersecurity mission for systems within their PO. The ISSO(s) for each PO is responsible for ensuring that an appropriate security posture is maintained for the information systems within their responsible charge. The ISSO is the principal advisor on all technical matters involving system security, should have detailed, in-depth knowledge of the information systems, and plays an integral role in continuous monitoring.

The key responsibilities for the ISSO are to:

- Serve as the primary point of contact and coordination within the PO for IA/cybersecurity matters
- Ensure that system user understand his/her IA/cybersecurity responsibilities by tracking user completion of Department IA/cybersecurity training and awareness
- Support management within a PO with the required IT security planning and budgeting
- Ensure that security patches for all IT systems are installed within the timeframe of the Information Security Vulnerability Management (ISVM) message published by the EDCIRC Coordinator, and are documented in accordance with the Configuration Management plan.
- Report and respond to IA/cybersecurity incidents, in accordance with the Department's OCIO-14 *Information Security Incident Response and Reporting Procedures*

- Remain current on the duties pertinent to the roles and responsibilities of an ISSO.

2.8 Users

Authorized users of Department IT resources, including all government employees and contractors, either by direct or indirect connections, are responsible for complying with the Department's IA/cybersecurity policy and security-related guidance. Their responsibilities include:

- Complying with the Department's IA/cybersecurity policy and security-related instructions and guidance
- Complying with security training and awareness sessions, commensurate with their roles and responsibilities
- Reporting any observed or suspected security issues to their supervisor, the Helpdesk, ISSM, ISSO, EDCIRC, or EDSOC

Certain information systems within the Department contain information that is open to the public. For this document, unless explicitly indicated otherwise, members of the public are not considered "users."

3. POLICY RESPONSIBILITIES, ORGANIZATIONS, AND DOCUMENTS

The purpose of this chapter is to identify the security controls applicable to all Department systems. The controls in this section are defined at a high level and are primarily supported by a security control standard that provides specifics for the controls. These controls were derived from Federal laws, OMB policies, NIST Special Publication 800-53, and Department IA/cybersecurity requirements.

3.1 FISMA, FIPS-199, and OMB Circular A-130

The Federal Information Security Management Act of 2002 (FISMA) requires all Federal departments and agencies, to provide cybersecurity controls and functions for their information systems. Under FISMA, the Federal Information Processing Standard (FIPS) 199 requires that all Federal Systems be categorized as to their security sensitivity in the areas of confidentiality, integrity, and availability, to arrive at an overall sensitivity categorization.

NIST SP 800-53 describes the concept of "Common Controls" - cybersecurity controls that are centralized in a support system and provide protections as a service to systems. The use of common controls relieves the individual system of some of the burden of providing its own IA/cybersecurity controls, and also helps ensure the consistency and uniformity of the controls. SP 800-53 also

describes the concept of "Hybrid Common Controls," which require active coordination between the support system that provides the control and the system which receives the services.

The Office of Management and Budget Circular A-130, Appendix 3, *Security of Federal Automated Resources* establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and, links agency automated information security programs and agency management control systems.

3.2 FISMA Reporting

FISMA requires that the Department report on the cybersecurity status of each of its Systems on regular periodic schedules. Although FISMA itself does not contain explicit criteria specifying systems reporting requirements, the implicit intent is that "FISMA-reportable" systems include all systems that have any impact on Department's overall security posture and not just systems that process, store or transport sensitive information.

For each FISMA-reportable system, the PO that owns the system has the responsibility for providing the needed information to address any FISMA reporting requirements.

3.3 Capital Planning and Investment Control

All Department Systems must be accounted for in the Department's Capital Planning and Investment Control (CPIC) reporting process. This process is administered by the Investment and Acquisition Management Team (IAMT) in the IT Program Services Group of OCIO, and is necessary to integrate and identify funding for information security technologies and programs into IT investment and budgeting plans. Integration of IA requirements for any system into the CPIC is critical for the success of the IA/cybersecurity program.

Exhibit 300 Section E of OMB Circular No. A-11, Part 7 addresses security and privacy issues with respect to IT capital asset investments relating to the enhancement, development and/or modernization of an agency's systems, both planned and operational. For further details on this security control area, please refer to OMB A-11*, Preparation, Submission, and Execution of the Budget,* and NIST Special Publication 800-65: *Integrating IT Security into the Capital Planning and Investment Control Process*

3.4 Security Authorization

Security Authorization refers to a formal analysis conducted by the PO to verify that the identified set of security controls are present and fully operational in the IS, and that this set of controls is sufficient to protect the system and data to the

full extent required by law and Department policy. Once the analysis of a system has been completed, the Authorization is granted for the system to advance to an operational status.

To implement the Security Assessment and Authorization:

- The PO has the responsibility for the selection, use, tailoring, verification and monitoring of all applicable controls for each IS. The PO documents the process in the System Security Plan (SSP, a component of the Security Authorization package), which describes fully the application of all cybersecurity controls to the IS

- After verifying that all cybersecurity controls and functions work properly in the IS, the PO creates a Security Test and Evaluation (ST&E) Report

3.5 Risk Assessment and Management

The PO system owner shall assess the risks to their systems and information, as part of an ongoing Risk Management Framework (RMF) approach, used to determine adequate security for a system by analyzing the threats and vulnerabilities, and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level of risk. Please refer to the Risk Management Framework guidance for details regarding this iterative process.

3.6 Critical Infrastructure Protection (CIP)

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7) addresses the identification of the Nation's critical infrastructure and the responsibility of any Department or Agency that possesses any component of critical infrastructure to provide for its protection, assured availability, and correct functioning.

Responsibility for interpretation and implementation of HSPD-7 falls within the purview of the Department's Office of Management (OM) in consultation with the CIO and other appropriate personnel.

3.7 Protection of National Security Information

All classified national security Information entrusted to ED shall be handled in accordance with OM-01: *Handbook for Classified National Security Information,* as well as other applicable Federal laws and standards. OM is responsible for establishing appropriate controls regards the creation, processing, storage, transmission, handling, marking, and disposal of classified information, and shall ensure that only individuals with the appropriate clearances and a need-to-know are allowed access to any classified information.

3.8 Records Management

The National Archives and Records Administration (NARA) and GSA have both established records management program regulations for the permanent retention of official Government records. The POs that own Systems are responsible for ensuring that the appropriate record retention and disposition schedules are followed. They must ensure that master records can be recovered in the event records are damaged or inadvertently erased.

OM has the responsibility for the Department's Records Management program, and documents. OM: 6-103, *Records and* Information *Management Program,* and OM: 6-106 *Records Retention and Disposition Schedules* shall be used to ensure compliance with the Department's Records Management program.

3.9 Lifecycle Management

Lifecycle Management (LCM) is the structured approach to managing IT projects. The responsibility for implementing LCM for Department Systems rests with the PO that develops the IS. All IA processes that involve the development, acquisition, implementation, maintenance, and disposal of IT solutions shall be assigned to the LCM framework. See Department document OCIO: 3-108, *Information Technology Investment Management (ITIM) and Software Acquisition Policy* for more information.

Security life cycle planning shall be integrated into the Department's capital planning and investment control process. Department document OCIO: 1-106, *Lifecycle* Management *Framework* shall be used to incorporate the security practices of the Department's information security program. The documentation of the LCM is the responsibility of the PO that owns the IS, and is included in the component of the Systems Security Authorization package.

3.10 FIPS-200 and NIST Special Publication 800-53

FISMA requires all Federal departments and agencies to provide security controls for their ISs. Under FISMA, FIPS 200 cites the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 as the minimum standard and best practices for these cybersecurity controls. NIST SP 800-53 identifies "Families" of cybersecurity controls to address the requirements of FISMA.

SP 800-53 is periodically revised by NIST to reflect the latest information on Government Cybersecurity policy, technologies, and threats. When a new revision becomes final, it is automatically binding on all Civil-Federal Departments and Agencies for the purpose of satisfying FISMA. Therefore, in the document, all references to SP 800-53 refer the latest revision that is then current

3.11 Access Control

FISMA and FIPS 200 require that all users of Government Systems be identified, and that their identities be authenticated before they are allowed to access the systems. It is the Department's policy to limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems), and to the types of transactions and functions that authorized users are permitted to exercise.

The responsibility for implementation and enforcement rests jointly with the POs that own the Systems and data and the Personnel Security office of the Office of Management (OM/PS).

3.12 Identification and Authentication

FISMA requires that all users of Federal systems, before being allowed access to the systems, be positively identified as having previously been granted access to those systems. FISMA further requires that the claimed identity of each user be authenticated in such a way that the authentication; (i) is reasonably resistant to impersonation, forgery, or other misuse; and, (ii), possesses strength and assurance that is commensurate with the sensitivity of the assets being protected. Identification and authentication standards should follow current requirements as defined by NIST and Homeland Security Presidential Directives.

3.13 Physical and Environmental Security

FISMA and OMB guidance require physical and environmental security for all Federal Systems in order to protect their operations. Physical and environmental security is normally provided as common controls, protecting all Systems within a particular processing site.

All Department POs shall follow the physical security guidance established in Department of Education, OM: 4-114, *Physical Security Program*. Facility managers shall implement applicable security guidance and controls identified in NIST SP 800-53 in Department data centers and facilities.

In the case of facilities and areas that are owned by contractors, the contractors shall be required, in their contracts, to provide physical and environmental security controls that are similar to those required for Government facilities. The ISSO who administers such facilities shall be granted full and continuing access to all assessments, visitor logs, and all other documents necessary to verify and monitor the efficacy of these controls.

3.14 Personnel Security

All Department POs shall follow the personnel security requirements outlined in the most current versions of: *OIG-1: Handbook for Personnel Security Suitability*

Program, and OM: 5-101, Contractor Employee Personnel Security Screenings. Additionally, all POs shall (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

3.15 Continuity of Operations, Disaster Recovery, and Contingency Plans

FISMA requires that all Federal departments and agencies create, implement, and periodically test plans for ensuring the continuity of operations of all Department mission-essential functions in the occurrence of threat events, including natural and man-made disasters (e.g., weather events, fire, flood, earthquake, civil disturbance), equipment failures, and cyber events such as network failures or system penetrations. The Department has a Continuity Plan of which one component is continuity of operations plan (COOP). The Department's Continuity Plan is not responsible for mandating a subset of cybersecurity controls and functions. This is to be identified in the Disaster Recovery (DR) plan. Additionally, each PO is responsible for the development of a Business Continuity Plan (BCP) that outlines the PO's continuity strategy and ability to perform their essential functions. OCIO is responsible for the identification of critical systems in coordination with POs and OM/SS to ensure performance of essential functions during a continuity event.

The responsibility for the COOP rests with the Continuity Manager in coordination with the Continuity Coordinator and is described in the document OM 5-102, *Continuity of Operations Program*. The responsibility for DR rests with the relevant PO, and is described in the individual PO's DR Plan. For each individual IS, the PO that owns the system shall create a Contingency Plan (CP) that confirms that the controls in the COOP and DR (whether common or specific to the IS) are sufficient to provide COOP and DR protection to the IS.

3.16 Internet Use and Controls

FISMA and OMB have instituted a number of requirements regarding the use of the Internet by the government. These requirements (and their associated policies) are of three types**:**

- Requirements that affect the overall architecture of the Department cyber facility, in particular to segregate public-facing Systems (especially public use web sites in the ".gov" domain) from Systems intended solely for official, internal use. The implementation of these requirements rests with the OCIO and is described in the documents containing the overall Department cyber facility architecture. In those cases where the facility is managed by a

contractor, the facility is required to provide architecture and protections that are equivalent to those of Government-owned facilities, and the architecture information is contained in the contractor's facility documentation

- Requirements from OMB and the Federal Network Resiliency (FNR, within the Department of Homeland Security) that mandate all Federal connections to the Internet to pass through Trusted Internet Connections (TICs)

- Requirements that concern cooperation between Department and the US Computer Emergency Response Team (US-CERT). These requirements address the reporting and monitoring of, and response to, cyber-attacks that originate on the Internet. The Department /US-CERT cooperation also includes Department participation in US-CERT Continuous Monitoring efforts such as the Common Vulnerability Enumeration (CVE) and the Common Platform Enumeration (CPE)

All aspects of Department /US-CERT cooperation are the responsibility of the IAS, and are detailed in the document developed by the IAS Cyber Security Operations organization.

3.17 The Privacy Act, Privacy Assessments, and System of Records Notices

The Federal Privacy Act and OMB Circular M-03-22 require all Federal departments and agencies to actively identify and protect specific types of private information that may exist in any of their systems. Primarily, the question is whether the system processes, stores, or transmits Personally Identifiable Information (PII) about individuals. The formal definition of PII is contained in OMB Circular M-03-22, but generally, PII is information that can be used to identify a specific individual. The protections mandated for PII are intended to ensure the confidentiality of PII, although they can affect integrity as well.

Ensuring conformance to the Privacy Act is the responsibility of the Department's Chief Privacy Officer, and the process for doing so is addressed in ACS Directive OM: 6-104. The analyses conducted by the PO shall follow OM:6-104 and consist of (i) a Privacy Threshold Assessment (PTA), to determine whether the system stores, processes, or transmits PII, (ii) if the system does handle PII, a Privacy Impact Assessment (PIA) will determine what IA/cybersecurity controls are needed to protect it. The results of the PTA and the PIA (if applicable) will be included in the SSP as part of the Authorization package.

The Privacy Act also requires that any system must be declared a "System of Records" if it meets all of the following:

- Contains information about individuals that is retrieved by an individual's name or other unique identifier

- Contains at least one personal identifier (such as name, SSN, or date of birth) by which the information can be retrieved
- The information is retrieved via name or other personal identifier.

3.18 Remote Access and Telework

Remote Access refers to any instance in which users are allowed access Department data and functional assets from any point outside of the physical security perimeter of an authorized Government facility, or a facility of an authorized contractor. Examples of remote access include (i) access to Department Systems by equipment vendors or by Government employees for the purpose of performing maintenance or diagnostics; (ii) Government or contractor employees accessing Department Systems from home or other remote locations to perform routine work; (iii) authorized access to Department Systems by non-Department partners such as other Federal departments, state and local governments or other organizations; or (iv) access by the general public to information that has been specifically designated as publically available.

Telework refers to Government or contractor employees conducting normal components of their work assignments from remote locations, such as working from home.

All forms of remote access, including telework, must have security protections that equal or exceed those that are provided within the Department's own physical security perimeter.

3.19 Interconnection Security and Computer Matching Agreements

An interconnection is a direct connection of two or more IT systems from different organizations, such that the software initiates the transfer of data from one system to another. (This does not include manually-initiated transfers such e-mail or manual file transfer protocols.) When one of the Systems resides with Department and the other does not, FIPS 200 and NIST SP 800-53 require that the two organizations that own the Systems establish and enforce an Interconnection Security Agreement (ISA) that details the IA responsibilities of each party. An ISA is also required if both organizations reside within the Department, but do not have identical security policies, or the Systems are not administered by the same PO.

A special case occurs when either or both of the interconnected Systems processes, stores, or transmits PII, or are Systems of Records, or both. In these cases, the Privacy Act requires additional documentation called a Computer Matching Agreement (CMA). The CMA ensures that the overall use of the PII or of the System of Records between the two systems is still consistent with the

Privacy Act. CMAs must also conform to Department Directive OM: 6-105, *Computer Matching Agreements*.

Each request for an ISA/CMA shall be prepared by the PO(s) that owns the Department-resident system(s), and shall use NIST SP 800-47, *A Security Guide for Interconnection Information Technology Systems* as guidance. If one of the correspondent Systems resides outside of Department, the ISA must conform to Department Directive OPEPD: 1-101, *Interagency Agreements*.

3.20 Cloud Computing

NIST SP 800-45 defines “cloud computing” as: a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The Department requires that system owners: (i) use FedRAMP when conducting risk assessments, security authorizations, and granting ATOs for all Department use of cloud services; (ii) use the FedRAMP PMO process and the JAB-approved FedRAMP security authorization requirements as a baseline when initiating, reviewing, granting and revoking security authorizations for cloud services; (iii) ensure applicable contracts appropriately require Cloud Service Providers (CSPs) to comply with FedRAMP security authorization requirements; (iv) establish and implement an incident response and mitigation capability for security and privacy incidents for cloud services in accordance with.DHS guidance; (v) ensure that acquisition requirements address maintaining FedRAMP security authorization requirements, and that relevant contract provisions related to contractor reviews and inspections are included for CSPs; and (vi) consistent with DHS guidance, require that CSPs route their traffic, such that the service meets the requirements of the TIC program.

3.21 Configuration Management

Configuration management establishes the appropriate configuration settings on information systems and technologies to provide adequate security to protect computing resources. Requirements to establish mandatory configuration settings derive from the Federal Information Security Management Act as implemented by FIPS 200 and NIST Special Publications 800-128: *Guide for Security-Focused Configuration Management of Information Systems,* and 800-53 (*Security Control CM-6, Configuration Settings*), and OMB Policy.

PO system owners shall: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

3.22 Incident Response

An incident response and reporting capability serves as a mechanism to receive and disseminate incident information, and also provides a consistent capability to respond to incidents as they occur. The National Institute of Standards and Technology (NIST) Special Publication 800-61: *Computer Security Incident Handling Guide* defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."

Incident response has become necessary because attacks frequently cause the compromise of personal and government data. Incidents involving viruses, worms, Trojan horses, spyware, and other forms of malicious code have disrupted or damaged millions of systems and networks around the world. Social engineering and other techniques attempt to coerce an individual into providing sensitive information to include username and password, bank accounts, and personally identifiable information (PII) through phone calls, emails and attachments, and bogus websites. Other incidents involve intentional or unintentional misuse of sensitive data, to include PII, through transmission in unencrypted emails or attachments, copies left unattended on desks or shared copiers/printers, and inappropriate disclosure to individuals without a need to know. These events—and many more—make the case daily for responding quickly and efficiently when computer security defenses are breached.

Suspected security breaches must be reported to EDSOC and EDCIRC following reporting procedures found in OCIO-14, *Handbook for Information Security Incident Response and Reporting Procedures.* Suspected PII breaches should be reported to the Principal Office's ISSO who will report it to the EDSOC and EDCIRC.

3.23 Awareness and Training

FISMA and OMB guidance require that all Federal departments and agencies ensure that their personnel receive annual security awareness training, and for employees with specific security job roles and functions, annual role-based training is required.

The Department mandates that all personnel and supporting contractors receive training prior to accessing Department information systems on an annual basis. This training focuses on raising the awareness of security risks associated with

their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems. The Department further requires that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. For further details on this security control area, please refer to the most current version of ED *IT Security Awareness and Training Program Guidance*.

3.24 Wireless and Mobile Device Security

The OCIO shall monitor and manage government-furnished and personally owned mobile and wireless electronic devices used for government business purposes.

At the ED Computer Incident Response Capability (EDCIRC) Coordinator's discretion, all mobile and wireless electronic devices used for government business purposes are subject at any time to:

- Possible sanitization (deletion of all data from mobile and wireless device(s))
- Re-setting of mobile and wireless device(s) to Department-approved, default settings

For further details on this security control area, please refer to the most current versions of the Department's *Wireless and Mobile Computing Guidance*, and the *Mobile Electronic Device Security Guidance*.

APPENDIX A: DEFINITIONS

Authorization To Operate	See Security Authorization (To Operate).
Authorizing Official (AO)	A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Controlled Unclassified Information (CUI)	A category of information the Department manages that is not covered by the National Security Act, but the unauthorized disclosure, alteration, or unavailability of which could have negative ramifications for the Department, its customers, or its business partners, or cause a loss of public confidence. This type of information is intended for use within the Department or within affiliated organizations such as Department business partners. This information may contain the labels “Controlled Unclassified Information”, “Sensitive But Unclassified Information”, or “Privacy Act Protected Information,” but is still considered CUI. Disclosure of this information to, or alteration by, unauthorized individuals is against laws, directives or regulations, and due diligence is required to protect it.
Exception	A case to which a rule does not apply. For example, a system owner may request an exception to a policy requirement.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that an Executive agency uses in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
System	A system is equipment that is (1) owned, leased, or operated by the Department (2) operated by a contractor on behalf of the Department or (3) operated by another Federal, state, or local Government agency on behalf of the Department.
Personally Identifiable Information (PII)	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Privacy Impact Assessment (PIA)	A formal statement regarding any system whose Privacy Threshold Assessment (PTA) has determined contains Personally Identifiable Information (PII). The PO that owns the system prepares the PIA, details the PII contained in the system, and stipulates any additional cybersecurity controls that are required in the system to protect the PII.
Privacy Threshold Assessment (PTA)	A formal statement regarding a system that asserts whether or not the system processes, stores, or transmits PII. The PO that owns each system must create a PTA for each one. If the PTA determines that PII is present, then the PO must create a PIA for the system.
Security Authorization (To Operate)	The official management decision made by a senior agency official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. See Authorization To Operate.
Sensitive But Unclassified (SBU)	Information that is sufficiently sensitive that its confidentiality, integrity and availability must be protected by security measures, but which does not fall under the purview of the National Security Act.
System of Record Notice (SORN)	A notice published in the *Federal Register* indicating that an IT system under Federal control allows retrieval of records by the name of an individual or by individually identifiable information.
System Security Plan (SSP)	A document that provides an overview of the security requirements of systems and describes the controls in place or planned for meeting those requirements. The SSP also delineates responsibilities and expected behaviors of all individuals who access the system.
User	Any person or organizational or programmatic entity that uses or receives service from an automated information system facility. A user may be either internal or external to the agency responsible for the facility.

APPENDIX B: ACRONYMS

ACS	Administrative Communications System
AO	Authorizing Official
ATO	Authorization To Operate
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
EARB	Enterprise Architecture Review Board
EDCIRC	ED Computer Incident Response Capability
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GSA	General Services Administration
GSS	General Support System
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IAS	Information Assurance Services
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
MA	Major Application
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OIG	Office of Inspector General
OM	Office of Management
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PO	Principal Office
PMI	Personnel Manual Instruction
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
SBU	Sensitive But Unclassified
SORN	System of Records Notice
SSP	System Security Plan
US-CERT	United States Computer Emergency Response Team

APPENDIX C: REFERENCES

The following list generally provides the high level governance documents covering Department cybersecurity. A complete list is located at *URL on ConnectED*.

Federal Laws and Regulations:

- E-Government Act of 2002 including Title III Federal Information Security Management Act (FISMA), P.L. 107-347
- Information Technology Management Reform Act, P.L. 104-106 (Clinger-Cohen Act of 1996)
- Privacy Act of 1974, as amended, 5 U.S.C. § 552a
- Federal Financial Management Improvement Act of 1996 (FFMIA), September 1996
- Federal Manager's Financial Integrity Act of 1982 (FMFIA), September 1982
- Electronic Communications Privacy Act of 1986, October 1986

Executive Orders and Memorandums:

- Executive Order 13556: *Controlled Unclassified Information (CUI*), November 2010
- Executive Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013
- Executive Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006

Office of Management and Budget (OMB) Circulars:

- OMB A-11*, Preparation, Submission, and Execution of the Budget,* August 2012
- OMB A-123, *Management's Responsibility for Internal Controls*, December 2004
- OMB A-130, *Management of Federal Information Resources*, November 2000
- OMB A-130, Appendix III, *Security of Federal Automated Information Resources*
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

- OMB M-06-15, *Safeguarding Personally Identifiable Information (PII)*
- OMB M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006
- OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007
- OMB M-08-05, *Implementation of Trusted Internet Connections (TIC)* November 20, 2007
- OMB M-09-02, *Information Technology Management Structure and Governance Framework*, October 21, 2008

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications:

- FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*, May 2001
- FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

NIST Special Publications (SP):

- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- NIST SP 800-30, *Guide for Conducting Risk Assessments*, September 2012
- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Feb. 2010
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, May 2013

- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010

- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories, Vols. I and II,* August, 2008.

- NIST SP 800-61, *Computer Security Incident Handling Guide*, October 2008

Department of Education Policy:

- OCIO: 1-104, *Personal Use of Government Equipment,* April 16, 2008

- OCIO: 1-106, *Lifecycle Management (LCM) Directive Framework,* July 16, 2010

- OCIO: 3-108, *Information Technology Investment Management (ITIM) and Software Acquisition*, March 4, 2010

- OCIO-15, *Handbook for Protection of Sensitive But Unclassified Information*

- OIG-01, *Handbook for Personnel Security-Suitability Program*, November 30, 1992

- OIG:1-102 *Cooperation with and Reporting to the Office of Inspector General*, January 9, 2014

- OM: 3-104, *Clearance of Personnel for Separation or Transfer*, June 26, 2008

- OM: 4-114, *Physical Security Program*, January 29, 2008

- OM: 5-101, *Contractor Employee Personnel Security Screenings*, July 16, 2010

- OM: 6-103, *Records and Information Management Program*, January 30, 2007

- OM: 6-104, *Privacy Act of 1974 (Basic Requirements) and the Collection of Personal Information*, August 31, 2006

- OM: 6-105, *Computer Matching Agreement*, January 22, 2007

- OM: 6-106, *Records Retention and Disposition Schedules*, November 16, 2007

- OM: 6-107, *External Breach Notification Policy and Plan*, April 15, 2008
- OPEPD: 1-101, *Interagency Agreements,* October 14, 2008
- PMI 368-1 *Personnel Manual Instruction*, March 14, 2007