ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

CYBERSECURITY POLICY

DEPARTMENTAL DIRECTIVE ACSD-OCIO-004

Distribution:
All Department of Education Employees

Approved by:
Denise L. Carter
Acting Assistant Secretary, Office of Finance and Operations

Approved on:
04/12/2019

History of Changes

Approved by	Notes	Date
Denise L. Carter Acting Assistant Secretary, Office of Finance and Operations	Superseded Handbook OCIO-01, Information Assurance Cybersecurity Policy, dated January 18, 2017.	04/2012/2019
Vanessa Tesoriero Directives Management Officer	No substantive changes. Technical changes: Sec. 508 accessibility compliance updates	01/21/2022
Vanessa Tesoriero Directives Management Officer	No substantive changes. Technical changes: Update contact; renumbered per new ACS document numbering system; Sec. 508 accessibility compliance updates	01/12/2023

VANESSA TESORIERO

Digitally signed by VANESSA TESORIERO
Date: 2023.01.12 08:43:31 -05'00'

For technical questions regarding this directive, please contact please contact Information Assurance Services (IAS) at OCIO_IAS@ed.gov .

Table of Contents

I. Purpose 1

II. Authorization 1

III. Applicability 2

IV. Policy 3

V. Responsibilities 4

Appendix A: Authorities 23

I. Purpose

The U.S. Department of Education (ED)'s Office of the Chief Information Officer (OCIO) Cybersecurity Policy (henceforth "Policy") provides direction to all ED employees, contractors, and any individual who receives authorization to access ED data, information technology (IT) systems, or systems maintained on behalf of ED to assure the confidentiality, integrity, and availability of ED information and systems.

As the Federal agency responsible for establishing policy for, administering and coordinating most Federal assistance to education; ED collects, uses, protects, discloses, maintains, and stores personal and other sensitive information and data subject to Federal law, regulation, and guidance.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), ED has established an Enterprise-wide Information Security Program (ISP) to safeguard the confidentiality, integrity, and availability of its information and systems.

This Policy defines the structure under which ED protects and controls access to EDs information and information systems. The ED Chief Information Officer (CIO) and the ED Chief Information Security Officer (CISO) jointly developed and maintain this policy document. This Policy requires all ED stakeholders, including Business Owners and Information System Security Officers (ISSOs), to implement adequate information security and privacy safeguards to protect all ED information.

II. Authorization

The Policy is based on legislative, statutory and executive directive requirements that include Federal laws and regulations, Presidential Directives and Executive Orders, Federal IT Acquisition Reform Act (FITARA), FISMA, the National Institute of Standards and Technology (NIST) Special Publications (SP) 800 series, the NIST Federal Information Processing Standards (FIPS), and Office of Management and Budget (OMB) memoranda. ED has an obligation under Federal Law and from the White House (Executive Branch) mandate to define and operate an effective cybersecurity program. At a minimum, this requirement is driven by:

A. Public Law No: 113-283 (12/18/2014), commonly known as the FISMA, amends the Federal Information Security Management Act of 2002. It directs agency heads to ensure that: (1) information security management processes are integrated with budgetary planning; (2) senior agency officials, including chief information officers, carry out their information security responsibilities; and (3) all personnel are held accountable for complying with the agency-wide information security program.

§ 3553. Authority and functions of the Director and the Secretary, Part (a), Subpart (2) requires agencies: "to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of —

1. Information collected or maintained by or on behalf of an agency; or
2. Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency".

§ 3554. Federal agency responsibilities, Part (a), Subpart (7) requires: "(b) AGENCY PROGRAM. — Each agency shall develop, document, and implement an agency-wide information security 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".

B. OMB Circular A-130, Section 3. Applicability

The requirements of this Circular apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government. The requirements of this Circular apply to management activities concerning all information resources in any medium (unless otherwise noted), including paper and electronic information. When an agency acts as a service provider, the ultimate responsibility for compliance with applicable requirements of this Circular is not shifted (to the service provider). Agencies shall describe the responsibilities of service providers in relevant agreements with the service providers.

C. Appendix I to OMB Circular A-130, Section 3. General Requirements, Part b:

1. Protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for their confidentiality, integrity, and availability; and
2. Provide adequate security for all information created, collected, processed, stored, transmitted, disseminated, or disposed of by or on behalf of the agency, to include Federal information residing in contractor information systems and networks.

Refer to Appendix A for a more complete list of applicable authorities.

Violation of this policy provided herein may result in disciplinary and/or legal action.

III. Applicability

The Policy directs all ED employees, contractors, and users that are authorized with access to ED information systems, or systems operated or maintained on behalf of ED, or ED information. 'Information' means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. Information System Owners (ISOs) shall work with the ED Chief Information Officer (CIO) and Chief Information Security Officer

(CISO) as required tailoring the policy requirements to any special case community of non-student users of ED and Federal Student Aid (FSA) IT systems.[1]

IV. Policy

All ED information must be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction—whether accidental or intentional — in order to maintain confidentiality, integrity, and availability. The security and privacy controls that provide this protection must meet Federal requirements with additional risk-based and business-driven control implementation achieved through a defense-in-depth[2] security structure. Access to all ED information must be limited based on a least-privilege[3] approach and a need-to-know basis. OFO-O: 5-101 will determine personnel security screening requirements for contractor employees who will require access to ED information, data, IT systems, and/or ED facilities or space. United States citizenship is requited for all Moderate Risk/Public Trust or High Risk/Public Trust or National Security designation positions. Requests to waive this policy requirement must be submitted and approved by OCIO/IAS and Director, Office of Security, Facilities and Logistics Services (OSFLS). Authorized user access must be limited to only information necessary for the performance of required tasks.

Information security is an enterprise-wide and individual responsibility that is shared by Senior Agency Officials, all ED managers and staff, Business/ Information/System Owners, IT professionals, and all other users of ED information and information systems. ED must implement an Enterprise-wide ISP that provides policies, instructions, standards, and guidance to ensure the protection of its information and information systems. ED must develop and maintain the information security policies and associated cybersecurity instructions for the ISP. The ISP will communicate overall ED cybersecurity policy, instructions, and supporting practices to assist senior ED officials and Business/Information/ System Owners on specific information security, such as management, operational, and technical safeguards.

Policy Structure

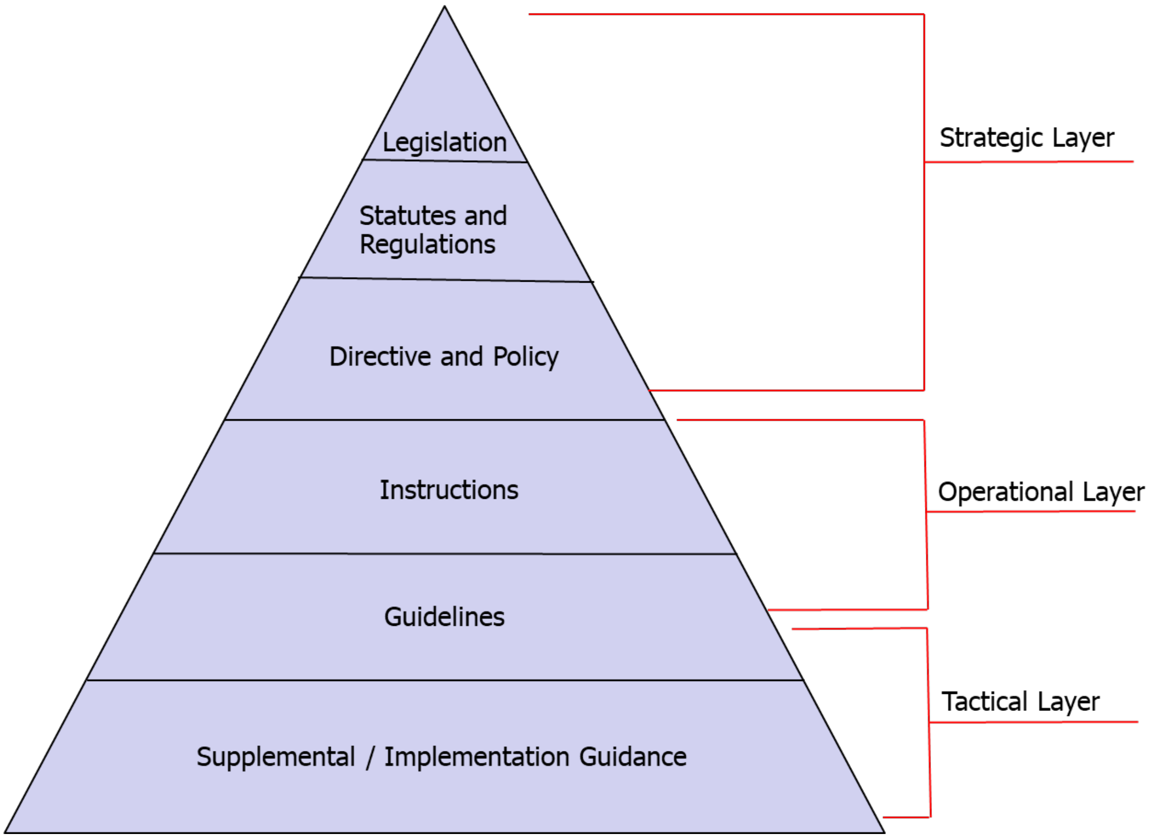
The structure of this policy framework is illustrated in Figure 1 below. It illustrates a framework that fully supports the strategic, operational, and tactical level needs of the ED for all cybersecurity policy

[1] Special case communities are instances of individuals who are not government employees or government contractors, but still require access to ED information systems to support the mission, function, and services of the ED. Some examples are school financial aid officers, third parties, grantees, and other external business partners

[2] [2] The Principle of Defense-in-Depth is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

[3] Offering only the required functionality to each authorized user, so that no one can use functions that are not necessary.

Figure 1 – Department Information Security Program Policy Hierarchy



V. Responsibilities

This section details significant information security roles and responsibilities for ED stakeholders.

A. General Roles

1. Federal Employees and Contractors (All Users)

All users have the responsibility to protect ED's information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction by complying with the information security requirements maintained in this Policy, ED CIO Cybersecurity Instructions and Standards. The responsibilities of users include but are not limited to the following:

a) Comply with all cybersecurity training and awareness requirements by the required due date, and role based training commensurate with their roles and responsibilities as needed;

b) Report any observed or suspected security issues to their supervisor, the ISSO, ED Security Operations Center (EDSOC), Contracting Officer (CO) and Contracting Officer's Representative (COR) if applicable; and

c) Conduct their daily operational tasks and work with proper security diligence and adhere to all applicable guidance disseminated under the ISP.

2. Supervisors

The responsibilities of supervisors are inclusive of item a. above and in addition include, but are not limited to, the following:

a) Notify the appropriate information security point of contact of any potential information security circumstances that impact users under their supervision; and

b) Ensure personnel under their direct supervision complete all required information security training, including privacy and Role Based Training (RBT), within the mandated timeframe as needed.

B. ED Federal Executives

This section describes the information security responsibilities of ED Federal Executives, including the Secretary, Deputy Secretary, Office of the General Counsel (OGC), Office of Inspector General (OIG), Office of Finance and Operations (OFO), Office of the Chief Information Officer (OCIO), and Personnel and Physical Security Officers (PPSOs).

1. Secretary

The Secretary is responsible for:

a) Delegating information security responsibilities to the Deputy Secretary.

b) Provides information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of:

(1) Information collected or maintained by or on behalf of the ED; and

(2) Information systems used or operated by ED, by a contractor of ED, or other organization on behalf of the agency.

c) Complies with the requirements of FISMA and related policies, procedures, standards, and guidelines, including:

(1) Information security standards promulgated under section 11331 of title 40;

(2) Operational directives developed by the Secretary of Homeland Security under Section 3553(b); and

(3) Policies and procedures issued by the Director, Office of Management and Budget.

d) Ensures that information security management processes and technical requirements are integrated with ED strategic, operational, and budgetary planning processes.

e) Ensures that senior ED officials provide information security that is consistent with the ISP for the information and information systems that support the operations and assets under their control.

f) Delegates authority to ensure compliance with the law to the ED's Chief Information Officer (CIO), who in turn is required to designate a Senior Agency Information Security Officer to carry out the CIO's responsibilities and authority for management of ED information security programs, along with the authority to ensure compliance with the requirements imposed on ED under FISMA.

g) Ensures that the CIO is fully empowered to initiate any contractual oversight, reform, or modification that is needed to ensure full compliance with the FITARA.

2. Deputy Secretary

Acting on behalf of the Secretary through delegation, the Deputy Secretary oversees the OCIO execution of the ISP to ensure it manages cybersecurity risk and improves the efficiency, effectiveness, and security of operations.

3. Assistant Secretary, Office of Finance and Operations (OFO)

The Assistant Secretary for the OFO is responsible for the following:

a) Plans, develops, implements, evaluates, and operates ED's Identity Document (ID) media program and the U.S. Government Personal Identity Verification (PIV) card program;

b) Ensures that individuals meet ED's personnel security requirements as well as HSPD-12 requirements for issuing U.S. Government PIV ID;

c) Issues IDs, while ensuring that ED's IDs are issued only upon review of personnel security files and in coordination with the Chief of Personnel Security and Disaster Preparedness. Implements PIV card hardware based authenticators, and personal identification numbers (PIN) and passwords that are compliant with FIPS publications; and

d) Establishes and provides processes and procedures for the validation of personnel clearances in support of Logical Access Control (LAC).

4. General Counsel

The Office of the General Counsel is responsible for providing counsel and legal assistance to the Secretary, Deputy Secretary, Directors, and ED's employees concerning the programs and policies of ED.

5. Inspector General

Pursuant to the Inspector General Act of 1978, as amended, 5 U.S.C. app., the OIG is charged with promoting the efficiency, effectiveness, and integrity of ED's information security programs and operations. The OIG conducts independent and objective audits, investigations, inspections, and other activities to evaluate ED's security program compliance with established Federal laws, regulations, and Directives, and to assess the effectiveness of its operation.

C. ED Information Security Officers

This section describes the information security responsibilities of those Federal employees with roles related to establishing this Policy and the associated Information Security Program designed to protect ED information and information systems.

1. Chief Information Officer

The ED CIO is the designated Senior Accountable Official for IT Risk Management. The CIO is the person formally authorized to assume responsibility for operating a system at an acceptable level of risk. The responsibilities of the CIO also include but are not limited to the following:

a) Serves as the Authorizing Official (AO) for all ED systems and approves information system Authority To Operate (ATOs) and denies ATOs, if identified risks are deemed to be unacceptable;

Federal Student Aid (FSA) will have delegated authority to authorize and approve FSA systems with the exception of any High Value Assets (HVAs) and systems with High and Moderate FIPS199 security categorization which must be approved by the ED CIO.

All High Value Assets (HVAs), General Support Systems (GSS), Inter-Agency Agreement (IAAs), High and Moderate FIPS199 security categorization systems must be authorized and approved by the ED CIO, however, low risk systems can be authorized and approved by a delegated authority of the ED CIO.

In recognition of the Inspector General Act, the Department's Inspector General will appoint an Authorizing Official for all OIG information systems and services as necessary.

b) Develops and maintains an ED-wide information security program;

c) Responsible and empowered in the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions, along with the management, governance and oversight processes related to IT;

d) Designates a senior ED Information Security Officer to develop and maintain an agency-wide ISP in accordance with FISMA 2014, and carries out the CIO's responsibilities for the ISP. (The senior ED Information Security Officer is also referred to as the Chief Information Security Officer (CISO);

e) Ensures that both the Deputy CIO, ED CISO, and other designees are empowered to take any action, in the absence of the actual CIO, by proxy, to ensure full compliance with FITARA for any areas that can be delegated and in compliance with Federal Regulations;

f) Defines mandatory information security and privacy training, education, and awareness activities undertaken by personnel, including contractors, commensurate with identified roles and responsibilities where applicable;

g) Publishes CIO Cybersecurity Instructions as required to augment existing policy;

h) Coordinates with other senior ED officials and core and essential enterprise cybersecurity programs (e.g., FICAM, HSPD-12, etc.), for reporting annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

i) Ensures that senior ED officials, including chief information officers of Federal Student Aid or equivalent officials, carry out responsibilities under this Subchapter, as directed by the official delegated authority by the Secretary of Education;

j) Manages and certifies an inventory of all current and proposed investments containing an IT component in accordance with the ED Capital Planning and Investment Control (CPIC) process; and

k) Ensures that all personnel are held accountable for complying with the agency-wide information security program.

2. Deputy Chief Information Officer (DCIO)

The DCIO is authorized to act on behalf of the CIO in the CIO's absence and is responsible for ED's daily information technology operations.

3. Chief Information Security Officer

The ED Chief Information Security Officer (CISO) operates under the direction and supervision of the ED CIO and the DCIO. The ED CISO is designated by the CIO as ED's Senior Agency Information Security Officer with the responsibility to develop and maintain an agency-wide ISP in accordance with FISMA 2014, and carry out the CIO's responsibilities for the information security program. The ED CISO is responsible for the development, implementation, effectiveness, and oversight of the ED's cybersecurity program in accordance with the cybersecurity mission. As part of this oversight, the ED CISO will determine the level of information security necessary to protect the ED's information in accordance with FISMA and for compliance to other national requirements and mandates.

The responsibilities of the ED CISO include but are not limited to the following:

a) Develops and maintains the ED-wide ISP as delegated by the ED CIO. Leads ED in the protection of information and information systems;

b) Improves ED's security posture by assuring the protection and integrity of its information and information systems through the implementation of Federal compliance standards, policy, and governance;

c) Coordinates the design and implementation of the processes and procedures needed to assess, quantify, and qualify risk with respect to ED's information resources; maintains information security procedures and control techniques that address all applicable information security requirements in ED;

d) Reports compliance status with program-related Federal mandates to Department leadership, the Department of Homeland Security (DHS), the Office of Management and Budget (OMB) Government Accountability Office (GAO) and/or Congress;

e) Implements information security awareness training to inform ED personnel and non-ED entities of the security risks inherent in operating ED's automated information systems;

f) Reviews any requested waivers and deviations from this Policy, Cybersecurity Instructions, or Cybersecurity Directives and provides recommendations to the AO/CIO for risk acceptance;

g) Acts as the authority to approve system configuration deviations and delegates the authority to the ISSOs, where appropriate;

h) Leads and coordinates the investigation and resolution of information security incidents and breaches across ED:

(1) Serves as ED's liaison with the United States Computer Emergency Response Team (US-CERT), OIG, and other external law enforcement agencies concerning information security incident reporting and follow-up activities;

(2) Coordinates incident response and threat information sharing with all Security Operation Centers (e.g., the FSA SOC and/or vendor SOCs), as appropriate;

(3) Defines and oversees the goals and requirements of ED Security Operations;

(4) Approves the appointments of ED ISSOs, except for FSA;

(5) Leads ED's cybersecurity risk management activities, including setting risk thresholds to maintain consistent risk acceptance decisions for ED's IT assets, information (data), services, operations, and individuals;

(6) Approves the independent security control assessment deliverables, except for the OIG;

(7) Coordinates with the CIO, OCO, PO Executives, ISSOs, and website owner/Administrator to ensure compliance with control family requirements (as per NIST 800-53) on website usage, web measurement and customization technologies, and third-party websites and applications; adherence to the current version of NIST SP 800-63, and satisfaction of the requirements in the current version of NIST SP 800-116; and

(a) Authorizes the immediate disconnection or suspension of any interconnection in the event of an incident;

(b) Coordinates with the Senior Agency Official for Privacy (SAOP) and Principal Office (PO) Executives to disconnect or suspend interconnections; and

(c) In coordination with the SAOP and the PO Executives, ensures interconnections remain disconnected or suspended until the Authorizing Official (AO) orders reconnection.

4. Senior Agency Official for Privacy (SAOP)

The SAOP is designated by the Department Secretary and is responsible for asset, data, and information privacy issues throughout ED. The SAOP is accountable for developing, implementing, and maintaining an ED-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, protecting, and disposal of Sensitive Personally Identifiable Information (SPII) and Personally Identifiable Information (PII).

5. Chief Privacy Officer (CPO)

The Chief Privacy Officer (CPO) supports the SAOP and is also accountable for developing, implementing, and maintaining an ED-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, protecting, and disposal of SPII and PII. The CPO has the following responsibilities:

a) Reviews and approves all ED Privacy Impact Assessments (PIAs) Privacy Threshold Analyses (PTA)s 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;

b) Implements ED's privacy program, including coordinating policy development, providing outreach and training, and working with OCIO to integrate safeguards for asset, information and data protection and system security;

c) Ensures that privacy is addressed throughout the life cycle of ED's information system, and that Federal privacy requirements are incorporated into the agency's enterprise architecture to ensure that risk is addressed and information systems achieve the necessary levels of trustworthiness, protection, and resilience;

d) Provides ED guidance and establishes security control assessment procedures for the implementation of privacy controls as specified in the current version of NIST SP 800-53, Security Controls and Assessment Procedures for Federal Information Systems and Organizations; and

e) Evaluates compliance of ED's systems against the current version of NIST SP 800-53 privacy controls and notifying the ED CISO and other appropriate authorities of instances of non-compliance.

6. Information Systems Security Manager (ISSM)

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

a) Advises the CISO, Information System Owners (ISOs), and Information System Security Officers (ISSOs) on asset, data, and information security risks associated with ED's current and planned information systems;

b) Ensures, through coordination with EDSOC, that all of ED's systems are in compliance with cybersecurity policy and reports the status to the ED CISO, Authorizing Official (AO/CIO) and ISSO;

c) Plans for and coordinates recurring and ad hoc meetings with ED's ISSOs to facilitate sharing of assets, data, and information, to communicate ED's cybersecurity priorities, and disseminate information regarding security awareness and training programs, and cybersecurity status of ED's information systems; and

d) Remains current on duties pertinent to roles and responsibilities of an ISSM.

D. Principal Office, Program, and Information System Roles

Principal Offices (POs) are components of ED responsible for a business area or mission. POs generally own a number of information systems and have major responsibilities in the protection of ED's assets, data, and information and the management of risk across its systems.

1. PO Executive

The PO Executive is the senior executive administratively and operationally responsible for all information systems assigned to the PO. The PO Executive has centralized responsibility for the establishment, maintenance, and enforcement of the information security program and policy for all information systems within the PO or business component. Although there are structural differences in the designation of a PO within the ED (specifically FSA), security-related responsibilities of the PO Executive include, but are not limited to:

a) Ensures that all security authorization activities for their assigned information systems are completed;

b) Ensures that an ISO and ISSO are designated for each PO information system and the ISSO designations are sent to the ED CISO for approval;

c) Ensures that ISOs and ISSOs within the PO have the necessary knowledge, skills, and abilities to perform their respective roles;

d) Maintains an up-to-date listing of the information systems and assets, and information (data) under their control and maintains awareness of the cybersecurity risk posture of each information system;

e) Ensure that ISOs adhere to cybersecurity requirements for all of ED's cybersecurity policies;

f) Manages personnel, assets, data, and information, and physical security matters within the PO;

g) Ensures that a PO-level asset, data, and information security continuous monitoring strategy is developed and implemented to enable ongoing visibility into the cybersecurity risk posture of each information system within the PO;

h) Notifies the ED CISO of any major changes to existing information systems or when planning the development of new information systems;

i) Ensures that all IT programs within the PO are properly resourced so that cybersecurity is fully incorporated throughout the program lifecycle;

j) Ensures that all PO information systems obtain an initial authorization to operate (ATO) and maintains a valid ATO throughout the information system lifecycle;

k) Ensures, in coordination with CORs and acquisition personnel, that cybersecurity is addressed in all IT-related procurements and contracts through appropriate language in requirements documents; and

l) Ensures current system inventories, system-level security plans, security reviews, corrective action plans, security authorization packages, and similar cybersecurity documents are developed, maintained, and posted to ED's system of record for FISMA reporting.

2. Federal Student Aid Chief Information Officer (FSA CIO)

The FSA CIO is the executive responsible for leading the Technology Office within FSA, and is the senior official responsible for the management of assets, data, and information resources within FSA, and their integration with ED's systems and data. The FSA CIO is subordinate to the ED CIO and develops, oversees, and manages FSA's cybersecurity mission and ensures that a risk management strategy is established and implemented. The FSA CIO has the responsibility for oversight of all risk related information and activities having FSA-wide impact and ensures that the information and/or activities are in alignment with the direction of ED’s CIO and the ED ISP. The FSA CIO’s significant security-related duties include:

a) Authorizes the FSA Deputy Chief Information Officer to act on their behalf when appropriate;

b) Designates the FSA CISO to execute FSA’s cybersecurity program;

c) Coordinates and integrates, where appropriate, through collaboration, all of FSA’s information assurance activities, with ED’s OCIO, and ED’s CIO;

d) Oversees the development and maintenance of FSA cybersecurity policy, procedures, and control techniques;

e) Ensures security considerations are integrated into FSA’s IT architecture, planning and budgeting cycles, and system development lifecycle management methodology;

f) Provides oversight, guidance, and support to FSA’s designated cybersecurity personnel;

g) Develops requirements to fulfill the cybersecurity responsibilities authorized by Federal law, regulations, and mandates for FSA;

h) Complies with Federal cybersecurity mandates;

i) Provides senior management input and oversight for cybersecurity risk management-related activities including risk acceptance decisions across FSA;

j) Develops and maintains cost estimates to secure adequate funding, resources, and training for the FSA cybersecurity program; and

k) Coordinates reports with the ED CIO for all reporting to OMB, the Department of Homeland Security (DHS), and others as required regarding the overall effectiveness of FSA’s cybersecurity programs, including progress of remedial actions; and manages the reporting processes under delegated authority provided by the ED CIO.

l) Ensures ED systems are utilized, in lieu of developing duplicative systems and services.

3. FSA Deputy Chief Information Officer (FSA DCIO)

The FSA DCIO is authorized to act on behalf of the FSA CIO in the FSA CIO's absence and is responsible for FSA's daily information technology operations.

4. Federal Student Aid Chief Information Security Officer (FSA CISO)

The FSA CISO is responsible for the development, implementation, effectiveness, and oversight of FSA's cybersecurity program, in accordance and alignment with the ED cybersecurity mission. The FSA CISO's responsibilities include:

a) Serves as the FSA CIO's principal point of contact for matters relating to the security of FSA's information systems and IT resources;

b) Coordinates and integrates all of FSA's information assurance activities, with ED's OCIO, and ED's CISO;

c) Collaborates with the ISOs to designate an Information System Security Officer (ISSO) for each FSA system and also approves the FSA ISSOs;

d) Executes the FSA CIO's cybersecurity responsibilities ;

e) Leads FSA's cybersecurity risk management activities, including setting risk thresholds to maintain consistent risk acceptance decisions for FSA's IT assets, information (data), services, operations, and individuals;

f) Advises the ED and FSA CIOs of any risks regarding information system vulnerabilities or issues that may have an adverse impact on FSA or the Department;

g) Ensures that FISMA performance metrics are coordinated with ED's CIO and CISO and that metrics are properly reported in a timely manner;

h) Coordinates information security incident reporting and emergency response activities throughout FSA, and with enterprise capabilities within ED; and

i) Aligns the FSA cybersecurity operations center capabilities to actively monitor and respond to FSA related cyber incidents in coordination with the EDSOC.

5. Information System Owner (ISO)

The ISO is formally designated by the PO and is responsible for the development, implementation, management, operation, security, associated security documentation, and continuous monitoring of assigned information systems to ensure that the operational interests of their user community are addressed.

ISOs manage the overall cybersecurity of their approved and assigned information systems and ensure that identified security vulnerabilities, policy, and mandate deviations are documented, reported, tracked and remediated on a POA&M. ISO responsibilities include:

a) Follows the guidance in ED’s Common Controls Catalog and the current version of NIST SP 800-53 and NIST SP 800-63, reviews information system documentation and the information system itself at least annually. If a major change/upgrade to the system occurs, the documentation would require updating for the information system as required in ED’s selected central cybersecurity repository (currently CSAM);

b) Ensures agreements are in place with internal and external entities when information systems share services, assets, or information and that the appropriate security contracting language are incorporated in each IT contract under their purview;

c) Ensures applicable portions of this policy are included in any user agreement necessary to gain access to ED information systems, services or ED data, which may include signed Non-Disclosure Agreements, Access Agreements, and appropriate Rules of Behavior;

d) Identifies residual risk and provides justification for AO risk decisions;

e) Drafts Privacy Threshold Analyses (PTAs) and PIAs and uses the Cyber Operations Branch, Office of the Chief Information Officer, PIA process to finalize and then post all PIAs to the ed.gov website as required under the E-Government Act of 2002;

f) Ensures that actions are taken to respond and complies within specified timelines for any government-wide or ED-wide directed action items related to vulnerability patching;

g) Ensures that periodic FISMA formal performance measure metrics reporting (quarterly and annually) are completed on time;

h) Signs off that system security designations are appropriately determined prior to system acquisition/procurement in accordance with FIPS 199 security categorization;

i) Processes systems at facilities that are certified at a level of security equal to or higher than the security level designated for their system;

j) Consults with ED’s OCIO and PO executives to establish consistent methodologies for determining information security costs for systems;

k) Ensures provision of adequate funding to implement the security requirements that fall within the management authority of the ISO;

l) Ensures that all IT systems under their purview are configured in accordance with most recent ED and Federal system security configuration guidance, and Federal CIO Council guidance (e.g., OMB M-11-11 and the Federal Identity Credential and Access Management Roadmap and Implementation Guidance);

m) Conducts assessments of the risk and magnitude of the harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the Department's critical operations, at no less than every three years or when significant changes occur to the system/network;

n) Ensures that system weaknesses are captured in the Plan of Action and Milestones (POA&M) and are entered into ED's selected Central Cybersecurity Repository (currently CSAM);

o) In coordination with the ISSO, ensures that sensitivity and criticality levels have been established for their systems and data in accordance with FIPS and NIST standards and guidelines;

p) In coordination with the ISSO, ensures proper physical, administrative, and technical controls are in place to protect PII if found in the system;

q) In coordination with the ISSO, ensures that security plans and authorization documentation for their system(s) and network(s) are developed and kept current for their system;

r) Obtains appropriate interconnection security agreements (ISAs) or memoranda of understanding (MOUs) prior to connecting with other systems and/or sharing sensitive data/information;

s) Ensures that system users and support personnel receive the requisite security training;

t) Determines who should be granted access to the system and with what rights and privileges, and grants users the fewest possible privileges necessary for job performance in order to ensure privileges are based on a legitimate need;

u) Conducts quarterly reviews and validations of system users' accounts to ensure the continued need for access to a system;

v) Enforces the concept of separation of duties by ensuring that no single individual has control of the entirety of any critical process in coordination with the ISSO;

w) Ensuring that special physical security or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk in coordination with the ISSO;

x) Ensures the development, execution, and activation of a system-to-system interconnection implementation plan for each instance of a system-to-system interconnection in coordination with the ISSO;

y) Collects, modifies, uses, and/or discloses the minimum PII necessary to accomplish mission objectives;

z) Notifies the ED CISO (FSA CISO included for FSA systems), ISSO and EDSOC of actual or suspected computer-security incidents, including PII and Protected Health Information (PHI) breaches; and

aa) Has an active security authorization for all deployed systems under the ISO's purview to include pilot systems and retiring systems, to include assembling the authorization package and submitting it to the AO or AO's Designated Representative; conducting quarterly reviews of applications or systems; and updating the data and information from quarterly reviews into ED's selected central cybersecurity repository (currently CSAM)

6. Information Systems Security Officer (ISSO)

An ISSO is responsible for ensuring that the appropriate operational security posture is maintained for an information system or program. Each information system will be assigned at least one ISSO. At FSA, the ISSO will be designated by a collaborative decision between the FSA CISO and the PO. All other ISSOs will be formally designated by the ED

CISO and PO. ISSOs are responsible for ensuring an appropriate security posture is maintained for their assigned information systems. The ISSO is the principal advisor on all technical matters involving information system security and should have detailed, in-depth knowledge of each assigned information system.

The key responsibilities of the ISSO include:

a) Follows the guidance found in ED's Common Controls Catalog and the current version of NIST SP 800-53, reviewing at least annually and updating the information system and information system documentation as required into ED's selected central cybersecurity repository (currently CSAM);

b) Serves as the primary point of contact for coordination of cybersecurity matters for their assigned systems;

c) Ensures that information system users required cybersecurity training is tracked;

d) Supports development of information system security planning and budgeting;

e) Ensures continuous monitoring of the information system's security is performed and validates the information system against the System Security Plan (SSP) while managing and controlling any information system updates;

f) Ensures that security patches for all assigned information systems are installed within the timeframe identified by ED policy;

g) Ensuring that all security related documentation for their systems are updated according to applicable guidance and standards;

h) Reports and responds to cybersecurity incidents in accordance with ED's Information Security Incident Response and Reporting Procedures;

i) In support of the ISO, ensures that actions are taken to respond and comply within specified timelines for any government-wide or ED-wide directed action items related to vulnerability patching;

This includes actions directed by the DHS, which issues "Binding Operational Directives" (BODs), that mandate reporting requirements by the Department for remediating critical vulnerabilities;

j) In support of the ISO, ensure that periodic FISMA formal performance measure metrics reporting (quarterly and annually) are completed on time and entered into ED's selected central cybersecurity repository (currently CSAM);

k) Ensures that information security notices and advisories are distributed to appropriate ED and contractor personnel and that vendor-issued security patches are expeditiously installed;

l) Ensures NIST SP 800-53 (as amended) controls are appropriate to the system based on the FIPS 199 security categorization;

m) Assists their applicable System Owner in capturing all system weaknesses, policy and standard deviations in the POA&M and entering them into the Department's selected central cybersecurity repository (currently CSAM);

n) Reinforces the concept of separation of duties by ensuring that no single individual has control of any critical process in its entirety per NIST SP 800-53 (as amended);

o) Tracks all information security education and awareness training conducted for personnel and contractors, as appropriate;

p) Limits information system access to authorized users, processes actions on behalf of authorized users, or devices (including other information systems);

q) Limits information system access to the types of transactions and functions that authorized users are permitted to execute;

r) Separates the duties of individuals to reduce the risk of malicious activity without collusion;

s) Employs the principle of least privilege, including for specific security functions and privileged accounts;

t) Uses non-privileged accounts or roles when accessing non-security functions, and;

u) Prevents non-privileged users from executing privileged functions and audit the execution of such function.

7. Contracting Officer (CO)

The ED CO responsibilities must include but are not limited to the following:

a) Ensures that all acquisitions, procurements and outsourcing efforts contain the appropriate information security requirement provisions and clauses that are consistent with ED policy;

(1) Ensures that performance work statements are routed through the OCIO IT governance process and

(2) Seeks attestation from the appropriate COR, ISSO or CISO as the subject matter experts that the identified security requirements are consistent with department policy.

b) Ensures that appropriate Service Level Agreements (SLAs) and underpinning contracts have been defined that clearly that clearly set out for the department a description of the service and the measure for monitoring of the service;

c) Ensures that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered; and

d) Ensures duties responsible for ED personnel security are outlined in Contracting Officer Representative letters.

8. Contracting Officer's Representative (COR)

The ED COR responsibilities must include but are not limited to the following:

a) Ensures the CISO, SAOP, and ISSOs are consulted during contract development and that the latest information security and privacy contract language is included in all contracts, as applicable;

b) Initiates and monitors background investigations and ensure that all users on their contracts comply with Federal and ED guidance for personnel security and background investigation requirements, and have taken security and awareness training before granting access to ED's systems and information;

c) Validates that all PIV and information security related contract language is incorporated into all acquisitions under their purview; and

d) Informs Personnel Security Office of any change to contractor personnel.

E. Privileged Users

This section describes specific information security responsibilities of users with privileged access to ED information systems. For example, a privileged user is any user that has sufficient access rights to modify, including disabling, controls that are in place to protect the system.

The responsibilities for all privileged users must include but are not limited to the following:

1. System/Network/Website Administrator

The responsibilities of the ED System/Network/Website Administrator include but are not limited to the following:

a) Implements proper system backups and patch management processes;

b) Assesses the performance of security and privacy controls associated with the system/network or web service to ensure the residual risk is maintained within an acceptable range and utilize PIV based authentication approaches;

c) Coordinates with the CIO, CISO, and ISSO to ensure compliance with control family requirements on website usage, web measurement and customization technologies, and third-party websites and applications; and

d) Limits connections to publicly accessible Federal websites and web services to approved secure protocols.

2. System Developer and Maintenance Administrators

The responsibilities of the ED System Developer and Maintainer must include but are not limited to the following:

a) Identifies, tailors, documents, and implements information security and privacy-related functional requirements necessary to protect ED information, information systems, missions, and business processes;

b) Ensures the requirements are effectively integrated into IT component products and information systems through purposeful security architecting, design, development, and configuration, following the ED change management processes;

c) Ensures the requirements are adequately planned and addressed in all aspects of system architecture, including reference models, segment and solution architectures, and information systems that support the missions and business processes;

d) Ensures automated information security and privacy capabilities are integrated and deployed as required and use PIV based approaches wherever possible;

e) Coordinates with the ISSO to identify the information security and privacy controls provided by the applicable infrastructure that are common controls for information systems;

f) Understands the relationships among planned and implemented information security and privacy safeguards and the features installed on the system;

g) Ensures ED systems or applications that currently disseminate data for any purpose are capable of extracting data by pre-approved categories; and

h) Shares only the minimum PII from ED systems and applications that is necessary and relevant for the purposes it was originally collected.

Appendix A: Authorities

Appendix A provides references to both authoritative and guidance documentation supporting the ED Cybersecurity Policy. Subsections are organized according to "level of authority" (e.g., Statutes take precedence over Federal Directives and Policies).

1. Statutes:

   - Federal Information Security Modernization Act of 2014 (FISMA 2014)
   - Information Technology Management Reform Act, P.L. 104-106 (Clinger-Cohen Act of 1996)
   - Privacy Act of 1974, as amended
   - Office of Federal Procurement Policy Act of 1974
   - National Cybersecurity Protection Act of 2014
   - Children's Online Privacy Protection Act (COPPA) of 1998
   - Government Paperwork Elimination Act (GPEA)

2. Federal Directives and Policies

   - OPM Regulation 5 Code of Federal Regulations
   - HSPD-7, Critical Infrastructure Identification, Prioritization and Protection, 2003
   - HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors
   -
   - Federal Information Systems Controls Audit Manual (FISCAM)
   - Federal Cloud Computing Strategy (Cloud-First), 2011

3. OMB Policy and Memoranda

   - OMB Circular A-130, Management of Federal Information Resources, 2000
   - OMB M-04-04, E-Authentication Guidance for Federal Agencies
   - OMB M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors

- OMB M-06-18, Acquisition of Products and Services for Implementation of HSPD-12
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 2007
- OMB M-10-06, Open Government Directive, 2009
- OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, 2010
- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, 2010
- OMB M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors
- OMB M-14-03, Enhancing the Security of Federal Information and Information Systems, 2013
- OMB M-15-13, Policy to Require Secure Connections across Federal Websites and Web Services, 2015
- OMB M-17-09, Management of Federal High Value Assets, 2016
- OMB M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program, 2018

4. Federal Information Processing Standards (FIPS) and NIST Guidance

- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, 1995
- NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, 1998
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Information Technology Systems, 2010
- NIST SP 800-35, Guide to Information Technology Security Services, 2003
- NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, 2010
- NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy, 2009
- NIST SP 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security, 2009
- NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport

Layer Security (TLS) Implementations, 2014

- NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems, including updates as of 1/15/2014, 2013
- NIST SP 800-53A Revision 4, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, 2014
- NIST SP 800-60 Revision 2, Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendice, 2008
- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide, 2012
- NIST SP 800-63 Rev 3, Digital Identity Guidelines
- NIST SP 800-100, Information Security Handbook: A Guide for Managers, 2006
- NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
- NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2018
- FIPS PUB 140-2, Security Requirements for Cryptographic Modules
- FIPS 186, Digital Signature Standard
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, 2006