



# ADMINISTRATIVE COMMUNICATIONS SYSTEM

UNITED STATES DEPARTMENT OF EDUCATION

Office of Management, Executive Office

400 Maryland Avenue; Washington, DC 20202

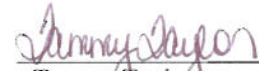
---

*Transmittal Sheet #:* 2006-0003 *Date:* March 31, 2006

*Distribution:* All ED employees

*Distribution Approved:*

*Directives Management Officer:*

  
Tammy Taylor

---

*Action:* Pen and Ink Changes

---

*Document Changing:* Handbook OCIO-01, *Handbook for Information Assurance Security Policy*, dated 12/19/2005

*Pen and Ink Changes:* The following pen and ink changes have been made.

---

<i>Page</i>	<i>Section</i>	<i>Changed</i>	<i>To</i>
All	Dates	12/19/2005	03/31/2006
1	Superseding Information	Information described above	Information described above
C1-C3	Appendix C	Updated links to references in Appendix C.	
Various	Various	Updated broken links throughout Handbook.	



ADMINISTRATIVE COMMUNICATIONS SYSTEM  
U.S. DEPARTMENT OF EDUCATION

## **DEPARTMENTAL DIRECTIVE**

**Handbook OCIO-01**

**Page 1 of 39 (03/31/2006)**

---

*Distribution:*  
All Department of Education Employees

*Approved by:* \_\_\_\_\_/s/\_\_\_\_\_(12/19/2005)\_\_\_\_\_  
Michell C. Clark, Acting Assistant Secretary  
Office of Management

---

### **Handbook for Information Assurance Security Policy**

---

For technical questions concerning information found in this ACS document, please contact  
Kathy Zheng on (202) 245-6447 or via [e-mail](#).

Supersedes Handbook OCIO-01, Handbook for Information Assurance Security Policy dated  
12/19/2005.

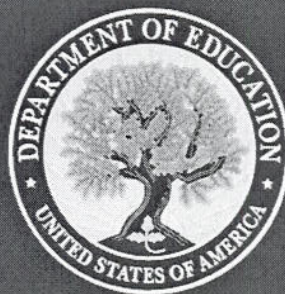
DEPARTMENT OF EDUCATION

Office of the Chief Information Officer

**Handbook for Information  
Assurance Security Policy**

Information Assurance Program

**March 31, 2006**



**Document Configuration Control**

Version	Release Date	Summary of Changes
Version 1.0	August 2004	Initial Release
Version 2.0	March 2005	ACS Review changes
Version 3.0	June 2005	ACS Final Document
Version 4.0	August 2005	ACS Release

As the U.S. Department of Education's (Department) Information Assurance Program evolves, this document is subject to review and update. Review and update will take place annually, or when changes that identify the need to revise the *Handbook for Information Assurance Security Policy* occur, such as changes in roles and responsibilities release of new executive, legislative, technical, or departmental guidance identification of a new policy area. The Director of Information Assurance Services or the Chief Information Officer, or both, must approve all revisions to the *Handbook for Information Assurance Security Policy*. The revisions are to be highlighted in the Document Configuration Control table. Each revised policy is subject to the Department's document review and approval process before becoming final. When approved, a new version of the *Handbook for Information Assurance Security Policy* will be issued, and all members of the team and affected groups will be informed of the changes made.

## Table of Contents

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1. Purpose .....	1
1.2. Scope.....	1
1.3. Document Organization and Structure .....	1
1.4. Enforcement .....	2
1.5. Exceptions .....	2
<b>2. SECURITY ROLES AND RESPONSIBILITIES .....</b>	<b>3</b>
2.1. Secretary of Education .....	3
2.2. Deputy Secretary of Education.....	3
2.3. Inspector General .....	3
2.4. Chief Information Officer (CIO).....	3
2.5. Critical Infrastructure Assurance Officer (CIAO) .....	4
2.6. Director, Information Assurance Services (IAS).....	4
2.7. Director, Information Technology Operations and Maintenance Services (ITOMS) .....	5
2.8. Director, Regulatory and Information Management Services (RIMS).....	5
2.9. Business Technology Advisor (BTA).....	5
2.10. Designated Approving Authorities (DAA) .....	6
2.11. Principal Officer .....	6
2.12. Computer Security Officer (CSO).....	7
2.13. System Security Officer (SSO).....	8
2.14. Network Security Officer (NSO).....	8
2.15. System Manager.....	9
2.16. Users .....	9
<b>3. MANAGEMENT CONTROLS .....</b>	<b>10</b>
3.1. Risk Management.....	10
3.2. System Security Plan .....	10
3.3. Information Technology (IT) Critical Infrastructure Protection (CIP) Program .....	10
3.4. Capital Planning and Investment Control .....	11
3.5. Contractors and Outsourced Operations.....	11
3.6. Review of Security Controls .....	11
3.7. Security Performance Measures .....	12
3.8. Certification & Accreditation (C&A).....	12
3.9. Privacy .....	12
<b>4. OPERATIONAL CONTROLS .....</b>	<b>14</b>
4.1. Personnel Controls .....	14
4.1.1. ... <i>Personnel Security and Suitability</i> .....	14
4.1.2. ... <i>Rules of Behavior</i> .....	14
4.1.3. ... <i>Acceptable Use</i> .....	14
4.1.4. ... <i>Access to Sensitive Information</i> .....	15
4.1.5. ... <i>Separation from Service</i> .....	15
4.2. Physical Security .....	16
4.2.1. ... <i>Sensitive Facility and Restricted Area Identification</i> .....	16
4.2.2. ... <i>Facility Access</i> .....	16
4.3. Contingency Planning.....	16
4.3.1. ... <i>Disaster Recovery and IT Contingency Planning</i> .....	16
4.3.2. ... <i>Documentation (Manuals, Network Diagrams)</i> .....	17
4.3.3. ... <i>Information and Data Backup</i> .....	17
4.4. Security Change Management .....	17
4.5. Lifecycle Management (LCM).....	18
4.6. Equipment Controls .....	18

4.6.1. ... <i>Hardware Maintenance</i> .....	18
4.6.2. ... <i>Software Maintenance</i> .....	18
4.6.3. ... <i>Wireless Security</i> .....	18
4.6.4. ... <i>Portable Electronic Devices</i> .....	19
4.7. Information Controls .....	19
4.7.1. ... <i>Data Sensitivity Classification</i> .....	19
4.7.2. ... <i>Information Protection</i> .....	20
4.7.3. ... <i>Information Marking</i> .....	20
4.7.4. ... <i>Media Sanitization</i> .....	20
4.8. Incident Response and Reporting .....	20
4.9. Security Training and Awareness .....	20
<b>5. TECHNICAL CONTROLS .....</b>	<b>22</b>
5.1. Identification and Authentication .....	22
5.1.1. ... <i>Identification and Authentication (I&amp;A)</i> .....	22
5.1.2. ... <i>Automatic Account Lockout</i> .....	22
5.1.3. ... <i>Passwords</i> .....	22
5.1.4. ... <i>Encryption</i> .....	23
5.2. Accountability .....	23
5.3. Access Control .....	23
5.4. Systems and Communications Protection .....	23
5.4.1. ... <i>Remote Access and Dial-In Access</i> .....	23
5.4.2. ... <i>Network Security Monitoring</i> .....	24
5.4.3. ... <i>Network Security Architecture</i> .....	24
5.4.4. ... <i>Network Connectivity</i> .....	24
5.4.5. ... <i>Warning Banners</i> .....	25
5.4.6. ... <i>Security Testing</i> .....	25
5.4.7. ... <i>Penetration Testing and Vulnerability Scans</i> .....	25
5.4.8. ... <i>Virus Protection</i> .....	26
<b>6. APPENDIX A: GLOSSARY .....</b>	<b>1</b>
<b>7. APPENDIX B: ACRONYMS .....</b>	<b>1</b>
<b>8. APPENDIX C: REFERENCES .....</b>	<b>1</b>

## 1. Introduction

### 1.1. Purpose

The purpose of this *Handbook* is to document and set forth the Department Information Assurance (IA) Security Policy. This IA Security Policy establishes policies required to comply with Federal laws and regulations, thus ensuring adequate protection on the Department Information Technology (IT) resources. The document is consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), the General Services Administration, and the Office of Personnel Management. At a minimum, the IA Security Policy includes the set of controls established by OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources and the security controls defined in NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information System.

The IA Security Policy contained in this document supports the Department's mission, goals, and objectives. This document is the primary source of policy and guidance that supports the IA Security Program in protecting the confidentiality, integrity, and availability of the Department's information that is collected, processed, transmitted, stored, or disseminated in its general support systems, major applications, and other applications. The policy described in this document is reinforced through a series of standards, directives, and other procedures documents that address specific aspects of the IA Security Policy. Those supplemental documents, which are referenced in Appendix C of this document, are to be used in conjunction with this *Handbook for Information Assurance Security Policy*.

### 1.2. Scope

The *Handbook for Information Assurance Security Policy* applies to all Department personnel and contractor support staff. The IA policy outlined in this document applies to all Department IT resources, including hardware, software, media, facilities, and data owned or in the custody of the Department. This IA policy supports the Department's IA Security Program objectives by identifying roles and assigning responsibilities in support of the Department's IA Security Program. In addition, the policy defines comprehensive and integrated security requirements that are necessary to obtain management authorization (accreditation) (See section 3.8) to allow the Department IT systems to operate within an acceptable level of security risk.

Security is a shared responsibility, and no single individual or position can be held responsible for the implementation of this policy. System-level requirements must be implemented by system security officers/system managers, but computer security officers, Principal Office officials, Office of Management and Office of the Chief Information Officer (OCIO) personnel all have a responsibility for ensuring identified controls are applied as required by this policy.

The Department's Baseline Security Requirements (BLSRs) and NIST SP 800-53, Recommended Security Controls supplement the policy in this document for Federal information systems, which have specific levels for application of security controls that fulfill these requirements. Additionally, the OCIO will issue further standards and procedures for the implementation for some of these controls.

### 1.3. Document Organization and Structure

The remainder of this document is organized as follows:

- Section 2** -- *Security Roles and Responsibilities*, defines roles and responsibilities associated with individual positions.
- Section 3** -- *Management Controls*, provides those policies that are related to managing the information assurance program, as well as the risk associated with operating the Department's IT systems.

**Section 4** -- *Operational Controls*, provides the requirements to be executed by the people that manage, operate, or use the IT system.

**Section 5** -- *Technical Controls*, provides the requirements for controls that must be implemented on the Department's IT systems.

In addition, this policy contains the following appendices:

- Appendix A - Glossary
- Appendix B - Acronyms
- Appendix C - References

## 1.4. Enforcement

Compliance with this IA policy is mandatory. This IA Security Policy requires all Department personnel and contractors that use the Department's IT resources to comply with the security requirements outlined in this document. Department personnel and support contractors' knowledge of and compliance with the IA policy contained in this document are critical to the successful accomplishment of the IA security program's goals and objectives.

Department personnel are found non-compliant with this policy may result in revocation of access to the Department's IT systems and data and may result in disciplinary actions. Contractors found not to be in compliance with this policy may have access to sensitive information revoked, may be required to agree to supplemental conditions of the contract, or may be forced to stop all work in support of the Department. Systems that fail to comply with this policy may not be allowed to process the Department information.

Enforcement and monitoring of this IA policy is the responsibility of the Department, Chief Information Officer (CIO). The CIO will review this policy annually or more often as needed and revise it to:

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

## 1.5. Exceptions

If compliance with any policy in this document is not feasible, technically impossible, or the cost of the control does not provide a commensurate level of protection, an exemption from that requirement may be provided. Exceptions shall be a decision made between the Business Owner and the Designated Approving Authority (DAA), in coordination with the CIO and/or the Director of Information Assurance Services (IAS).



## 2. Security Roles and Responsibilities

The roles and responsibilities described in this section are assigned to the positions identified to ensure effective implementation and management of the Department's IA Security Program. The establishment of a security management structure and assigning of security responsibilities is a requirement of OMB Circular A-130.

### 2.1. Secretary of Education

The Secretary of Education is responsible for the overall IA security program within the Department. In accordance with this responsibility, the Secretary is responsible for providing the oversight for developing and implementing the IT security policies, principles, standards, and guidelines that form the basis of a comprehensive IA Security Program. The Secretary also ensures that adequate funding for IT security is available.

### 2.2. Deputy Secretary of Education

Acting on behalf of the Secretary, the Deputy Secretary oversees the CIO's responsibilities in the development of IT security policies, standards, procedures, and guidelines for handling the Department's information and IT resources to improve the efficiency, effectiveness, and security of operations.

Significant security-related duties of the Deputy Secretary include:

- Providing oversight of the Department-wide IT security plan and information security policies
- Incorporating IT security principles and practices throughout the stages of the life cycles of the Department's systems.
- Ensuring that the CIO develops, implements, and oversees a comprehensive IT security program across the Department

### 2.3. Inspector General

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

In addition, under Federal Information Security Management Act (FISMA), the IG participates in providing a comprehensive annual review of the Department's IA program. The IG 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.

### 2.4. Chief Information Officer (CIO)

As the senior Department officer responsible for information resources management, the CIO ensures that the Department's IA Security Program is developed and implemented, both within the Department and with respect to external business relationships with other Federal agencies and external partners.

Significant security-related duties of the CIO include:

- Developing and implementing IA security policy across the Department
- Providing oversight and guidance for information and IT security-related activities within the Department

- Fulfilling the information assurance responsibilities assigned under PDD-63, the Clinger-Cohen Act, Executive Order 13231, and FISMA
- Serving as the overall Department certifier for all Department information systems, in support of the certification and accreditation (C&A) process, with the exception of the CIO's information systems
- Working with the Department's senior officers and staff to mandate and facilitate a secure information system operating environment throughout the Department
- Developing and maintaining reliable IT security cost estimates, which are used to secure adequate funding for the IA Security Program
- Ensuring implementation of the Department's IT Security Awareness and Training Program.

## **2.5. Critical Infrastructure Assurance Officer (CIAO)**

The security-related responsibilities of CIAO include ensuring the security of all Department cyber and non-cyber, mission-essential infrastructure assets.

## **2.6. Director, Information Assurance Services (IAS)**

The Director, Information Assurance Services, OCIO, is designated by the CIO and is responsible for the development, implementation, effectiveness, and oversight of the Department IA Security Program. Specific duties of the Director, Information Assurance Services, include:

- Providing oversight, guidance, and support to Department IT security personnel
- 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 General Support System (GSS) and Major Application (MA) inventory list
- 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
- Developing, establishing, and promulgating adequate IA security policies to ensure the confidentiality, integrity, and availability of the Department IT resources and data
- Ensuring that relevant security information, such as alerts, bulletins, and relevant communications, are passed to appropriate Department security personnel in a timely manner
- Assisting the Network Security Officers (NSO), CSOs, and Designated Approving Authorities (DAA) as necessary in IT security planning and budgeting
- Providing input to ensure that security is addressed in all information system-related procurements and contracts
- Overseeing and enforcing policy and guidance concerning the Department's Critical Infrastructure Protection (CIP) Program
- Overseeing and enforcing policy and guidance concerning the Department's C&A program

- Overseeing and providing direction to the Certification Review Group.

The Director, Information Assurance Services, serves as the central repository for all Department IT system security documents, including C&A documentation. The Director of IAS and the CIO may require changes to any such documents to ensure their completeness, consistency, and adequacy in meeting and conforming to Department IT security standards and policies.

## **2.7. Director, Information Technology Operations and Maintenance Services (ITOMS)**

The Director, Information Technology Operations and Maintenance Services, provides technical support to the CIO on matters related to the Department's network systems. Because of the Department's heavy reliance on the availability and integrity of its network systems, this position is critical in ensuring the overall IT security of the Department. Specific security-related duties of the Director, Information Technology Operations and Maintenance Services include:

- Providing guidance to Principal Offices on the technical security controls required to establish and maintain a secure architecture and operating environment for Department systems
- Establishing configuration management policy and procedures in conjunction with the Director, Regulatory and Information Management Services (RIMS), to ensure that proposed changes to the enterprise have been evaluated for their impacts on the overall security posture.

## **2.8. Director, Regulatory and Information Management Services (RIMS)**

The Director, Regulatory and Information Management Services, is responsible for planning, executing, and evaluating information management activities by the CIO and executes the following functions:

- Developing, monitoring, and maintaining the Department's RIMS policy, ensuring that the security aspects of information management are adequately addressed
- Providing guidance to the Director of IAS on the Department-wide data and hardware remanence policy
- Based on input from the Director of ITOMS and the Director of IAS, developing configuration management policy and procedures to ensure that proposed changes to GSSs and MAs have been evaluated for their impacts on the overall security posture
- Developing and maintaining the Department's Information Technology Architecture Framework and Information Technology Architecture Principles Guidance, which include guidance on IT security
- Providing guidance to the Director of IAS on the Department-wide privacy and e-mail issues related to FOIA, the Privacy Act, and the Federal Records Act
- Maintaining the Department's system inventory list, which includes the GSS and MA inventory from the Director of IAS; the EDNet technical architecture from the Director of ITOMS; and data collections.

## **2.9. Business Technology Advisor (BTA)**

As the assigned liaison to the Department's Principal Offices, BTA serves as liaisons to the full range of ITOMS, IAS, and RIMS services across OCIO. BTA responsibilities include:

- Gathering and communicating each office's unique IAS/ITOMS/RIMS requirements to the CIO
- Assisting in developing IAS/ITOMS/RIMS solutions tailored to mission and business processes

- Facilitating compliance with IAS/ITOMS/RIMS standards and performance measures.

In fulfilling these responsibilities, BTA ensures that security is addressed in information system-related procurements and contracts.

## 2.10. Designated Approving Authorities (DAA)

The DAA is recognized as the system owner and the management official with the responsibility to identify the level of acceptable risk for an information system or application and to determine whether the acceptable level of risk has been obtained. DAA responsibilities include:

- Reviewing and approving security safeguards of GSSs and MAs and issuing accreditation statements for each system within his/her Principal Office based on the acceptability of the security safeguards of the system
- Ensuring that an Interim Authorization To Operate (IATO) is granted only if the necessary security enhancements to bring the system up to the acceptable level of risk have been identified and a formal and timely plan for their implementation has been developed
- Coordinating system security requirements with the CIO, the IAS, and the DAA of other related and connected GSSs and MAs.

## 2.11. Principal Officer

The Principal Officer is the senior individual administratively and operationally responsible for all computer systems within the Principal Office 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 computer security 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 DAA for C&A activities are completed
- Maintaining an up-to-date listing of the GSSs and MAs under his/her control within the Principal Office
- 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 GSSs and MAs under his/her control or subject to his/her use
- Managing personnel, information, and physical security matters within the Principal Office
- Ensuring that a security self assessment<sup>1</sup> is completed for each GSS or MA at least annually that is consistent with the NIST SP 800-26 requirements and notify the Department's CIO of any changes
- Ensuring that all GSSs and MAs are certified and accredited in accordance with the Department's *Information Technology Security Certification and Accreditation Procedures*
- Ensuring, in coordination with the Director of IAS, BTA, and contracting officers, that IT security is addressed in all IT-related procurements and contracts

---

<sup>1</sup> If an independent risk assessment is completed within the annual timeframe and consistent with NIST 800-26, it may also meet the annual security assessment requirement.

- Ensuring current system inventories, system-level security plans, security reviews, corrective action plans, C&A packages, and similar IT security documents are developed and maintained and forwarded to the Director of IAS

## 2.12. Computer Security Officer (CSO)

The CSO is the individual formally designated by a Principal Officer to be responsible for the implementation and management of the IA security policy within the organization. Specific CSO duties include, but are not limited to

- Serving as the primary point of contact and coordination within the Principal Office for IT security matters
- Ensuring that the Principal Officer and the SSO for each IT system within the CSOs organization understands his/her IT security responsibilities, including matters that address IT security
- Serving as liaison between the Director of IAS and the Principal Office personnel responsible for IT security activities
- Within his/her Principal Office, supporting management relative to assisting them with the required IT security planning and budgeting for the Principal Office
- Ensuring that system users and support contractors throughout his/her Principal Office receive the requisite security awareness briefings, as described in the Department's *Information Technology Security Awareness and Training Program Plan*
- Monitoring and evaluating the security posture of all systems within the Principal Office, and reporting the status to the Principal Officer
- Ensuring the performance of a risk analysis for each information system installation and resource within his/her Principal Office, as described in the Department's *Handbook for Information Technology Security Risk Assessment Procedures*, and *NIST SP 800-30, Risk Management Guide for Information Technology Systems*
- Ensuring compliance with the Department's IA security policy for external information-processing activities (e.g., cross-servicing, computer matching, data sharing), whether conducted by or for the Government (see section 5.4.4)
- Maintaining a current list of all GSSs, MAs, applications, and facilities sponsored by his/her organization, and forwarding it and any related documentation to the Director of IAS upon request
- Preparing and maintaining C&A documentation for each GSS/MA under CSOs control for the Department's Certification Review Group
- Overseeing the development of a system security plan for all Principal Office systems
- Reporting fraud, waste, abuse, and suspicious activities concerning the Department IT resources
- Reporting and responding to IT security incidents, in accordance with the Department's *Handbook for Information Security Incident Response and Reporting Procedures*
- Performing other functions that may be required to ensure the integrity, confidentiality, and availability of the Principal Office's information system resources
- Ensuring that Principal Office staff and contractor support staff participate in and complete security awareness and specialized security training.

### 2.13. System Security Officer (SSO)

The SSO is responsible for implementing security policies and procedures for assigned GSSs and/or MAs. The SSO receives guidance from the CSO on security matters relevant to the assigned systems. SSO responsibilities include, but are not limited to, the following:

- Performing security-related activities for the assigned system in accordance with the guidance and direction of the CSO
- Developing, maintaining, reviewing, and updating comprehensive C&A documentation for the system on behalf of the business or functional manager, in accordance with NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*; NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*; and other Department guides, as applicable
- Maintaining an inventory of the hardware suite and software packages associated with the assigned system
- Managing the system password program in accordance with Department security policies
- Ensuring that adequate management, operational, and technical security controls are implemented and maintained on the system, and that these controls are tested regularly
- Performing an annual security assessment of the security posture of the system and reporting the status to the CSO

### 2.14. Network Security Officer (NSO)

The NSO is formally appointed by the Principal Officer for specific network for which the Principal Officer is responsible. The NSO is responsible for implementing the Department's security program for the network. NSO responsibilities include:

- Performing security-related activities for the network in accordance with guidance from the Director of IAS and the CSO
- Developing and maintaining a comprehensive security plan, along with other C&A documentation, for the network using *NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems* for guidance
- Managing the network password program in accordance with the Department security policies (password length, composition, aging, etc.)
- Ensuring that adequate management, operational, and technical security controls are implemented and maintained across the network, and that these controls are tested at least annually or whenever significant changes are made.
- Reporting security incidents to the CSO, as appropriate
- Monitoring and reviewing the security audit record and identifying and reporting to the Principal Officer, any inconsistencies or irregularities in network usage
- Performing an annual security self-assessment of the network and reporting status of the security posture to the Principal Officer
- Certifying to the DAA that the network security controls are in place, adequate, and functioning as designed to protect the information processed by the network

- Analyzing network software, hardware, and embedded technology devices for security compliance and ensuring that appropriate security patches are applied in a manner consistent with network configuration management policy

### **2.15. System Manager**

The system manager is the principal staff member responsible for the day-to-day operations of an IT system. The security-related duties of this individual include, but are not limited to

- Assisting the SSO in implementing the technical security controls of the system
- Reporting security incidents to the CSO, as appropriate
- Reviewing audit logs to identify system anomalies
- With the SSO, performing an annual security assessment of the system's security posture.

### **2.16. 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 IA Security Policy and security related guidance. Their responsibilities include:

- Complying with the Department IA security 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 problems/incidents to their CSO.

### 3. Management Controls

This section provides the basic management control statements for the Department IT systems and information and provides the foundation for implementing the operational and technical controls in the following sections. These management control statements are derived primarily from OMB Circular A-130 and NIST SP 800-53 and are integral to an overall IA security program. The manner in which these controls are implemented depends on the risks, sensitivity, and criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

#### 3.1. Risk Management

Risks associated with the Department's information assets shall be managed by the OCIO through development and implementation of a comprehensive risk management framework. The framework will include the establishment of an overall IA Program that addresses the following: IA Program Management; IA Policies, Standards, and Guidance; IA Operations Support; IA Training and Awareness; and IA Analysis and Assessment.

In support of the IA program, the OCIO will maintain a current and comprehensive list of all Department's IT systems requiring additional security considerations and will inventory those IT systems semiannually. Systems must be identified as general support systems, major applications, or applications following the procedures outlined in the Department's General Support Systems and Major Applications Inventory Procedures. DAAs shall implement a risk management process for all major applications and general support systems using *NIST SP 800-30, Risk Management Guide for Information Technology Systems* as a guide.

The security level designation will be assigned to a system based on the sensitivity of the system's data, the risks associated with the sensitivity of the system's data, and the operational criticality of data processing capabilities. Designation will occur following the procedures outlined in the Department's General Support Systems and Major Applications Inventory Procedures. The Department's risk management framework should be consistent with *NIST Federal Information Processing Standards (FIPS) Publication 199*, and *NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories*.

#### 3.2. System Security Plan

Pursuant to OMB Circular A-130, a system security plan is required for all major applications and general support systems. Security Plans shall be developed in accordance with *NIST SP 800-18, Systems Guide for Developing Security Plans for Federal Information Systems* and Department guidance. The plan must be reviewed by the Director of IAS and approved by the DAA before it is authorized to operate and process the Department's information (See section 3.8).

System security plans must be kept current and reviewed at least every three (3) years or whenever there is a significant change to the system. This may be completed as part of a system's risk assessment, certification review, or a separate documented event. This review may be done internally or through independent sources with results reported to IAS. IAS has developed the basic review criteria and reporting instructions that can be used to determine the compliance level.

#### 3.3. Information Technology (IT) Critical Infrastructure Protection (CIP) Program

Principal Offices are responsible for providing a level of protection for IT assets and information under their control, commensurate with the highest level of criticality associated with the asset. Asset owners must complete or update the Mission Essential Infrastructure (MEI) evaluation survey for each general



support system and major application under their control. This survey shall be completed semi-annually, or as directed by the CIO.

In coordination with the OCIO and the Office of Management (OM), Principal Offices shall analyze interdependencies of assets identified as essential and address any risks that are uncovered in the analysis.

Infrastructure dependencies not under the direct control of the Department must be protected through Memoranda of Understanding (MOU) with the entity that owns or has primary management responsibility for that infrastructure.

### 3.4. Capital Planning and Investment Control

In coordination with OCIO, systems owners shall integrate and explicitly identify funding for information security technologies and programs into IT investment and budgeting plans. All Departmental GSSs and MAs that meet OMB-established financial minimums shall be mapped to an Exhibit 300 and/or Exhibit 53, and shall have appropriate security budgeting and justification. Security costs identified in plan of action and milestones (POA&M's) shall be included in the respective Exhibit 300s and/or Exhibit 53s.

### 3.5. Contractors and Outsourced Operations

Principal Offices must ensure that third parties, including, but not limited to, vendors, contractors, and maintenance staff accessing their system resources and connecting to the Department IT systems, comply with all policies contained in this Department-wide *Handbook for Information Assurance Security Policy*. Specific security language regarding access shall be documented and incorporated into MOUs and into contracts, including physical controls, clearances required, data storage and use, and any other controls deemed necessary for the particular contract.

Contractor access to Department IT systems and information must comply with all current Department IA policies, including access to information and the requirement for security awareness training.

### 3.6. Review of Security Controls

System security officers/system managers shall ensure that a system security assessment is conducted annually. To meet this requirement, a system self-assessment must be completed in accordance with NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*.<sup>2</sup> If an independent risk assessment is completed within the annual timeframe and consistent with NIST 800-26, it may also meet the annual security assessment requirement.

In accordance with OMB Circular A-130, the Department's GSSs and MAs, including interconnecting IT systems, must undergo independent risk assessments of system controls at a minimum of every three (3) years or whenever significant changes occur. The type and scope of the review shall be commensurate with the acceptable level of risk established for the system. All such risk assessments shall be conducted in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, and Department's *Information Assurance Risk Assessment Guide*. All risk assessments must be documented and have signed acknowledgement of receipt by the system security officer and the Principal Officer.

Corrective actions for weaknesses identified through the assessments must be documented in the system's POA&M, including associated resources required for remediation.

---

<sup>2</sup> In response to the Government Information Security Reform Act (GISRA) requirement for an annual assessment, in July 2002, the Office of Management and Budget (OMB) required all non-national security systems to undergo a NIST SP 800-26 self-assessment on an annual basis. When FISMA superseded GISRA, the OMB requirement to use NIST SP 800-26 remained.

### 3.7. Security Performance Measures

The CIO shall collect information on the performance of security responsibilities and controls and determine sources and types of data to fulfill current and future Department objectives, including completing annual FISMA requirements.

The CIO shall also determine the timing of the collection, as well as the means employed. Department personnel shall comply with the direction provided by the CIO for the collection of security performance measures.

### 3.8. Certification & Accreditation (C&A)

All Department major applications and general support systems shall be certified and accredited prior to processing any Department information that has security considerations due to its confidentiality, integrity, or availability requirements. To be considered for authorization, system manager/SSO must complete the following:

- Risk Assessment Report
- Security Test and Evaluation
- Security Evaluation Report
- Contingency Plan
- System Security Plan
- Configuration Management Plan
- Plan of Action and Milestones (POA&M)

To receive authorization to process, the Designated Approval Authority (DAA) must accept the residual risk to a system after application of security controls.

All Department IT systems must be accredited at minimum every three (3) years and evaluated annually or whenever there is a significant changes<sup>3</sup> to the system's security posture. IT systems that are not major applications shall be certified and accredited as part of their general support systems or shall be combined with other systems. Ongoing monitoring of each system must take place in the interim years to ensure that any new security controls, minor system updates, and actions identified in the POA&M are applied and tracked. Any changes to the IT system or associated IT environment that affect the accredited safeguards or result in changes to the prescribed security requirements will require reaccreditation of that IT system.

The Director of IAS shall serve as the Department's repository for all official documentation required for C&A.

Under certain conditions, the Department may issue an Interim Authorization To Operate (IATO). After assessing the results of the security certification, if the DAA deems that the risk is unacceptable, but operation of the system is essential to fulfill the mission of the Department, an IATO may be granted. The IATO is a limited authorization under specific terms and conditions including corrective actions to be taken and a required timeframe for completion of those actions. An IATO shall be issued for no longer than six (6) months.

### 3.9. Privacy

All Department IT systems processing data that are protected under the Privacy Act must have measures implemented to protect personally identifiable information. Interconnecting systems owned by other departments and agencies that process the Department data must also be considered. Protection measures must consist of management, technical, and operational controls to ensure an acceptable level

---

<sup>3</sup> See Appendix A for a definition of 'significant change'.

of risk. An acceptable level of risk should be determined in accordance with the Department's Risk Management policy.

Personnel and contractors using the Department IT systems must be in compliance with the privacy policy. Systems owners shall complete a Privacy Impact Assessment for each GSS and MA within the Department.

## 4. Operational Controls

Operational controls concern requirements to design, maintain, and use Department systems in a secure environment. These security control statements are derived primarily from OMB Circular A-130 and NIST SP 800-53 and are designed to assist the Department personnel in providing security for IT systems and information on a day-to-day basis. The manner in which these controls are implemented depends on the risks, sensitivity, and criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

### 4.1. Personnel Controls

The application of the personnel policies below shall be coordinated with the actions of the Office of Management.

#### 4.1.1. Personnel Security and Suitability

All personnel and contractors accessing Department information and information systems shall undergo background screenings, as described in the Handbook (OIG-1) Personnel Security - Suitability Programs, prior to being granted access to the Department systems. All authorized users must be designated with a sensitivity level, based upon the requirements for the protection of information and IT systems for which that position is authorized. Consistent with the requirements of the Office of Management, Security Services, Personnel Security, and all personnel accessing the Department information must meet personnel security and suitability standards commensurate with their position sensitivity level and will be subject to personnel investigation requirements.

Personnel with security clearances are subject to a reinvestigation requirement if they continue to have a need for access to sensitive information.

#### 4.1.2. Rules of Behavior

Every Department general support system (GSS) and major application (MA) shall have specific Rules of Behavior that describe to the user those parameters in which they must operate to access the system; these Rules must be at minimum contained in the system security plan. Users must both accept and acknowledge the rules of behavior before being allowed access into any Department IT system or information. Rules of Behavior may include non-disclosure requirements.

The System Manager shall keep a record of users who have accepted and acknowledged the Rules of Behavior.

#### 4.1.3. Acceptable Use

##### 4.1.3.1. Software

- Users of Department IT resources shall use only software that is properly licensed and registered for the Department use.
- All Department users must abide by software copyright laws and shall not obtain, install, replicate, or use unlicensed software.
- Users of Department IT resources must obtain all software from the Department sources and shall not download software from the Internet without prior permission from the OCIO, as

downloading software from the Internet may introduce viruses/worms to the Department network.

#### 4.1.3.2. E-Mail

- Users shall use E-mail for Government business. However, users may occasionally make personal use of E-mail that involves minimal expense to the Government and does not interfere with Government business, and consistent with the Departmental directive on *Personal Use of Government Equipment*.
- Users shall not use E-mail for any activity or purpose involving classified data. All sensitive but unclassified data shall be protected via encryption and/or passwords, if possible.
- Users must avoid prohibited E-mail usages, including:
  - Transmitting unsolicited commercial announcements or advertising material, unless approved by management in advance
  - Transmitting any material pertaining to the Department, the Federal Government, or any Agency employee or official, that is slanderous or defamatory
  - Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, unauthorized mass mailings, or intentionally sending a virus/worm.

#### 4.1.3.3. Internet

- Personal use of Government IT systems for Internet access shall be kept to a minimum and shall not interfere with official system use or access, and consistent with the Departmental directive on *Personal Use of Government Equipment*.
- Users shall avoid prohibited Internet usages including:
  - Browsing sexually explicit or hate-based Web sites
  - Using Internet access for personal gain (i.e., making use of the Department resources for commercial purposes or in support of for profit activities such as running a private business)
  - Theft of copyrighted or otherwise legally protected material, including copying without permission
  - Sending or posting sensitive material outside of the Department network.

Detailed guidance regarding the Department personal use of government equipment is available at [Personal Use of Government Equipment](#).

#### 4.1.4. Access to Sensitive Information

IT systems must be assigned sensitivity levels for information stored, processed, or transmitted. The determination of whether an individual's official duties require access to sensitive information is to be made by the owner of the information.

Personnel who are granted access to sensitive information must have appropriate clearances and must acknowledge and accept the Rules of Behavior before being granted access. Non-disclosure requirements/agreements may be included as part of a system's rules of behavior. Personnel with access to sensitive information shall use only approved Department IT systems to process the information and shall not use personally owned equipment.

#### 4.1.5. Separation from Service

Supervisors shall notify system administrators within two (2) business days of the departure of employees and contractors; notification shall be immediate in the case of involuntary separation. System access for

voluntarily separated personnel shall be terminated as soon as possible, but no later than two business days of notification. Access for involuntarily separated personnel shall be revoked immediately. This applies to passwords, account user IDs, and all other access devices. When an employee or contractor's termination is processed, system administrators must be advised immediately by the designated supervisor to disable or delete all accounts.

A recent activity review of the outgoing employee will take place to inspect the information and IT systems the individual accessed prior to departure.

## 4.2. Physical Security

### 4.2.1. Sensitive Facility and Restricted Area Identification

Information Assurance Services, in conjunction with the Office of Management's Security Services, shall identify and designate sensitive facilities and restricted areas containing the Department information and IT systems. Following this designation, periodic assessment shall be conducted to ensure controls are in place and are properly implemented in a manner consistent with the Homeland Security Presidential Directive (HSPD)-12 and other policies and guidance issued by OMB.

### 4.2.2. Facility Access

Access to the Department's rooms, work areas/spaces, and data centers housing information or IT systems must be granted only to those who require access to perform their official duties. If the Department and facility physical security controls are insufficient, additional controls must be implemented.

Records of visitor access to these facilities shall be maintained and reviewed at least monthly to detect potential aberrations or anomalies.

## 4.3. Contingency Planning

### 4.3.1. Disaster Recovery and IT Contingency Planning

Contingency plans shall be developed and tested for all GSSs and MAs, in coordination with OMB A-130, Principal Office operations, and certification and accreditation requirements (See section 3.8) to ensure that the IT systems security controls continue essential functions if IT support is interrupted. All Department disaster recovery plans (DRP) and IT contingency plans shall follow established guidelines and be coordinated with the Continuity of Operations Plan and Business Continuity Plans they support. Contingency plans must be updated on an annual basis, at a minimum.

Critical and sensitive operations and supporting IT resources have been identified and prioritized through the efforts of the CIP and Continuity Services program. The identified critical and sensitive operations' data will be backed up according to the Department's Information and Data Backup procedures (See section 4.3.3).

All personnel involved in contingency efforts shall be trained in specific procedures and the logistics of their respective plans. Training shall take place annually or as significant changes to the plan are made.

Contingency plans must be tested and exercised at least annually, with results being documented and used to update the plans. Contingency plan test results and/or Corrective Action Plans (CAP's) shall be included as an appendix to the contingency plan.

#### 4.3.2. Documentation (Manuals, Network Diagrams)

Aspects of IT system support and operations must be documented to ensure continuity and consistency. Documentation for a GSS/MA must include, at a minimum:

- Descriptions of hardware and software (*If the application hardware or software are not within the boundaries of the MA, a reference shall be made to the GSS documentation that describes the hardware and software*)
- Privacy Impact Statements
- Policies, standards, and procedures (*specific to the system, provided by the system manager/SSO, that do not conflict with Departmental policy, standards and procedures*)
- Approvals for information processing
- Backup and Contingency Plans
- System Security Plans
- Configuration Management Plans
- Risk Assessments
- Security Testing and Evaluation
- Penetration Testing
- Disaster Recovery Plans

Additional documentation will be maintained based on the system requirements, sensitivity level, and specific needs of the Department offices.

Security documentation must be current and accessible to fulfill the needs of the different types of individuals who shall access and use it (SSO/system manager, CSO, the Director of IAS, etc.). This documentation must receive the same level of protection as the system or its information. Copies of critical system documentation such as the System Security Plans must be maintained in a secure location.

#### 4.3.3. Information and Data Backup

All IT systems shall have documented and implemented backup procedures. Backup media retention and media rotation shall be specified in the backup procedures, to be included in the System Security Plan for the IT system. Retention time should be appropriate to the sensitivity, criticality, and integrity requirements of the data and/or that which is required by law. It is the sole responsibility of the Department's employees and contractors to backup data on individual workstations.

The Department shall follow the National Archives and Records Administration (NARA) recommendation for electronic on-line and off-line storage as well as traditional paper (hardcopy) storage.

Backup data to be used for disaster recovery shall be stored at a secure off-site location and shall comply with the Department's Disaster Recovery and IT Contingency Planning (See section 4.3.1).

#### 4.4. Security Change Management

A system configuration management plan shall be developed, implemented, and maintained for every GSS and MA, to effectively manage and track configuration changes to each system managed by the Department.

The Director of IAS, in coordination with the Department CIO, the Director of ITOMS, and Program Offices, shall establish configuration management standards and guidance to ensure that proposed changes to the enterprise have been evaluated for their impacts on the security architecture.

## 4.5. Lifecycle Management (LCM)

All systems shall have adequate and effective management, operational, and technical control mechanisms integrated into the LCM from conception through disposal. Identification of new vulnerabilities and threats must occur throughout the LCM, and controls to mitigate those threats must also be identified and implemented.

All security considerations, including the rationale for not implementing required security safeguards, must be documented throughout the LCM in the system security and configuration management plans.

## 4.6. Equipment Controls

### 4.6.1. Hardware Maintenance

The availability and usability of the Department's equipment shall be maintained and safeguarded to enable the Department's objectives to be accomplished. Repairs, maintenance, or both, shall not cause any IT system to become unavailable to users unless approved by the Department's CIO's and/or the appropriate authorized personnel. Affected IT systems shall be backed up before maintenance or repair. Adequate notice of system unavailability must be given prior to taking systems off-line.

Only authorized personnel (e.g., system administrators, vendor technicians) are permitted to perform maintenance and repair activities on the Department hardware devices.

### 4.6.2. Software Maintenance

Personnel shall obtain permission from the OCIO to install personal or non-standard software on the Department computers and shall adhere to the Department's Acceptable Use Policy (See section 4.1.3) in using such software. All software installed on the Department IT systems must be appropriately licensed and registered for the Department use.

Maintenance shall comply with the system security plan, configuration management plan, and rules of behavior. Maintenance shall not cause any GSS or MA to become unavailable to users unless approved by the appropriate system owner(s)/IT System Manager(s). Affected IT systems shall be backed up before maintenance or repair.

### 4.6.3. Wireless Security

Unauthorized wireless networks, including wired or wireless components intended for establishing wireless connectivity to any Department system or network, are prohibited. Wireless networks or devices shall not be used for storing, processing, or transmitting classified information at all times. If a wireless service or wireless network connectivity is authorized, only assured channels employing approved encryption and authentication mechanisms shall be used to transmit classified information. All authorized wireless devices and connections that are integrated or connected to the Department networks are considered part of those networks, and must be in accordance with the Department's policy and procedures outlined in the Handbook for Telecommunications.

Unauthorized 'bridging' or the use of wireless devices to simultaneously connect with the Department owned networks and with other systems or networks, is strictly prohibited, without explicit written approval of the Director of IAS and the Director of ITOMS.



#### 4.6.4. Portable Electronic Devices

Portable Electronic Devices (PEDs) include, but are not limited to laptop computers with wireless capability, cellular/Personal Communications Service telephones, personal digital assistants, hybrid devices, one-way and two-way pagers, two-way e-mail devices, and other portable devices capable of storing, processing, or transmitting information.

PEDs are subject to the Department security evaluation processes and criteria. Department owned and issued PEDs may be used for processing the Department sensitive information, and may only connect to a Department computer system once a proper security evaluation has been conducted on the device, and the implementation, applications or programs are determined to comply with required security controls and have adequate help desk support. Department PEDs may only be used in the manner in which they have been explicitly authorized to be used.

All laptops requiring physical connectivity to an EDNet networking port must be configured to meet ED configuration standards. Laptops requiring such connectivity will not be allowed to connect to the Department's networks, systems, or applications without first being configured by the Department. All laptop equipment operated on or connected to EDNet must comply with the procedures outlined in the Department's *Use of Laptop Equipment on EDNet*.

Department PEDs are prohibited from connecting to a government computer system or computer network that processes Classified National Security information.

Individuals who have been issued a Department PED must report any misuse, loss, or theft of the wireless device immediately.

### 4.7. Information Controls

#### 4.7.1. Data Sensitivity Classification

Information handled by the Department is generally placed in two categories: "Unclassified" and "Sensitive But Unclassified" (SBU).

- Unclassified information requires no special handling and is available for public release.
- SBU data is strictly controlled on a need-to-know basis to preserve confidentiality and integrity. This group of data shall be evaluated by the user for its sensitivity level and handled appropriately, based on policies and procedures established by the Department, as well as applicable Federal laws.

Information that is determined to be "Confidential", "Secret" and/or "Top Secret", shall be handled in accordance to Handbook for Classified National Security Information and other applicable Federal laws and standards.

The CSO shall identify the level of protection required for a particular system commensurate with the need for confidentiality, integrity, availability, and accountability of the data processed by the system. The CSO shall make risk level determinations for positions required to handle data within Principal Offices. The determinations shall be in accordance with Federal and Departmental standards and policies. Where duties of the position involve more than one risk level, the higher risk level will be assigned to the position. Department contractors who are granted access to sensitive information must have appropriate authorization before being allowed access. Department personnel with access to information as delineated above shall use only approved Department IT systems to process the information and shall not use personally owned equipment.

#### 4.7.2. Information Protection

All sensitive information that is transmitted outside the Department network shall be protected. All media (e.g., diskettes, hard drives, zip drives, floppy disks, CD-ROMs, DVDs, flash drives, and tapes), including backup media, containing the Department information shall be protected in a manner commensurate with the sensitivity of the data. The receipt and delivery of media containing sensitive data shall be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit.

#### 4.7.3. Information Marking

All media (e.g., diskettes, hard drives, zip drives, floppy disks, CD-ROMs, DVDs, flash drives, and tapes), shall be marked according to the sensitivity and criticality of the information contained therein. In any case where media may contain data of various sensitivity and criticality, it shall be marked to represent the most sensitive and critical data contained therein.

Access to information shall be restricted to appropriate personnel (See section 4.7.1).

#### 4.7.4. Media Sanitization

To prevent the inadvertent release of the Department's sensitive data, magnetic media, diskettes, hard disks, or other storage devices containing the Department data or software must be sanitized prior to the transfer, reuse, or donation of any equipment or media. Sanitization methods shall be commensurate with the sensitivity and importance of data residing on storage devices or equipment. Media must be logged and tracked through final sanitization. When warranted, sanitation of media can also include destruction through shredding, pulping, degaussing, crushing, or pulverizing.

### 4.8. Incident Response and Reporting

Each employee and contractor of the Department is responsible for reporting suspicious events to the relevant CSO. All authorized users shall be trained to promptly report suspected vulnerabilities, security violations, and security incidents to their CSO and/or the ED Computer Incident Response Capability (EDCIRC) Coordinator.

All suspected security incidents shall be reported immediately to the CSO and all reported incidents shall be handled in accordance with the Department's Handbook for Information Security Incident Response and Reporting Procedures. To reduce the risk of sensitive information being released inappropriately, only authorized personnel should have access to the incident data. E-mails regarding a security incident, as well as documents such as incident reports, should be encrypted so that only the sender and intended recipients can read them. The Department will adhere to NIST guidance as set forth in NIST SP 800-61, Computer Security Incident Handling Guide, and subsequent publications. Criminal activity must be reported to the Office of the Inspector General Computer Crimes and Investigation Division (CCID).

### 4.9. Security Training and Awareness

A security awareness training program shall be established by the OCIO to ensure all Department personnel and contractors involved in the use of IT systems are aware of their responsibilities for safeguarding the Department's IT resources.

All Department personnel, including contractors who have access to the Department's information and information systems that support the operations and assets of the agency, shall fulfill the Department's information system security training program. IT Security Awareness and Training Guide outlines the Department's training policy, which can be summarized as follows:

- Information system security training is incorporated into the new hire and new contractor orientation processes. Training must be completed within ten (10) working days of employment or initiation of contract.
- All personnel and contractors shall complete annual information system security awareness refresher training.
- Information system security personnel with responsibilities related to administering and securing systems are provided with specialized security training applicable to their functions.
- Information system specialized security training may be in the form of classroom, computer-based, or other format, as determined by the OCIO.

The security awareness training cycle begins in August and closes in August of the following calendar year. Non-compliance with this training requirement will result in disciplinary action. The OCIO will continually update training courseware, curricula, and awareness initiatives to address evolving threats and vulnerabilities, and to reflect changes in Federal guidance, Department policies, and/or functional roles.

## 5. Technical Controls

This section provides the basic technical control security policy statements for the Department IT resources. Technical controls provide specific guidance on security mechanisms and technical procedures used to protect the Department IT systems and information from unauthorized access, use, disclosure, disruption, modification, or destruction. The control statements are derived primarily from OMB Circular A-130 and NIST SP 800-53 and are integral to an overall IA security program. The manner in which these controls are implemented depends on the risks, sensitivity, and criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

### 5.1. Identification and Authentication

#### 5.1.1. Identification and Authentication (I&A)

Proper controls must be implemented and maintained on the Department IT systems to confirm user identity prior to access. The access protection measures must provide assurance of individual accountability through identification and authentication of each IT system user. Audit logs of login attempts of critical networking systems or components, whether successful or failed, must be maintained and reviewed at least weekly. Auditing of log files of non-critical systems must be completed on a monthly basis where applicable (i.e., the system is inherently capable of auditing).

Administration of the authentication data must include procedures to disable lost or stolen tokens, smart cards, or passwords and include procedures for the recovery of cryptographic keys.

Individual authentication information must not be shared among users or system personnel.

The Director of ITOMS and Director of IAS will issue standards for the authentication process to ensure a uniform approach throughout the Department and in accordance to the controls imposed by FIPS 201. Additionally, the OCIO will provide further technical guidance in the implementation of electronic authentication (e-authentication).

#### 5.1.2. Automatic Account Lockout

All Department IT systems shall employ controls that lock users out after not more than three (3) failed login attempts.

All login attempts shall be recorded in an audit log and shall be reviewed according to the accountability and the Identification and Authentication policy.

Procedures must be in place for detecting, responding, investigating and responding to consecutive or suspicious failed login attempts.

#### 5.1.3. Passwords

All Department IT systems must implement password controls that prevent unauthorized access. Department users must maintain control of their password and protect it from inadvertent disclosure. It is the duty of all Department individuals to practice good password management procedures. Users must not share passwords. Where allowable (i.e., when certain legacy systems and applications can not meet this policy), passwords must be strong. Strong passwords must include three of the four characteristics; numeric and alphanumeric characters, upper and lower case letters and special characters. Passwords must be at least eight (8) characters in length. Passwords must not match or resemble the word

'password' in any form (as-is, capitalized, or adding a number, etc.). Users are not allowed to use anything pertaining to their names in any form (login name, first or last name).

Regular changing of passwords shall be systemically enforced in accordance with procedures outlined in the system security plan. Forgotten or compromised passwords must be replaced. Users must prove identity before a replacement password is issued.

#### **5.1.4. Encryption**

Department IT systems that identify the need for the use of encryption technology must include such controls in the system security plan. An IT system using cryptographic technology must have procedures documented in the system security plan describing cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, retrieval and archiving.

Use of encryption technologies, including public/private key cryptography, must conform to applicable NIST guidance. Encryption products approved by NIST will be used to protect IT systems and information.

The IAS shall establish standards and guidance for the proper use and implementation of encryption mechanisms for the storage, transmission, or processing of data on the Department IT systems.

### **5.2. Accountability**

When feasible (i.e., new systems and applications or non legacy systems and applications), all Department GSSs and MAs shall have implemented logging and auditing controls. System auditing procedures shall be established to record security events and actions of each user. System security officers/system managers must identify in the system security plan the responsible party for reviewing audit logs and the period for audit log reviews, which must be at least monthly. The length of time for which audit logs are to be maintained must also be included in the system security plan.

Access to audit logs must be restricted to designated system personnel.

### **5.3. Access Control**

All Department GSSs and MAs shall implement controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions and maintain a record of access to the Department IT system. These controls shall be implemented in a manner consistent with FIPS 201, NIST SP 800-53, and Departmental directives and other applicable Federal standards and guidance. These controls shall be documented in the system security plan.

Access to IT resources and records must be limited to authorized individuals. Access controls must follow the principle of least privilege and separation of duties.

### **5.4. Systems and Communications Protection**

#### **5.4.1. Remote Access and Dial-In Access**

Remote access to the Department's network must be conducted using the Department-provided or supported services. Remote access to the Department's network shall be granted only to individuals authorized by management to work from home or from other non-Department work sites. Accessing the Department's e-mail from home or from an alternate work site will not require to obtain remote access service permission.

The Director of ITOMS must approve all requests for dial-in access to the Department. Dial-in access is only granted when the compelling need has been established and a level of security commensurate with the risk to information accessed has been provided.

#### 5.4.2. Network Security Monitoring

The IAS shall create general guidelines and procedures for the approved methods of security monitoring on the Department networks.

Users shall not expect privacy on the Department IT systems. All activities on the Department IT systems are subject to monitoring by network administrators to the extent permitted by law and outlined under Department directives. Network monitoring will include network discovery for the detection of unauthorized/rogue devices, including but not limited to, modems, wireless access points and servers. Service monitoring may include e-mail, e-mail transmissions or attachments, Voice Over Internet Protocol (VOIP), Internet use, or any service provided by the Department. Monitoring may occur through traffic analysis, keystroke monitoring, examination of log files, and examination of any or all files on the computer. Monitoring shall take place regularly in accordance with procedures and when evidence of apparent misuse of possible criminal activity has been reported.

Department resources and data, user account and directories, user files, user e-mail, or other data may also be subject to review. Designated personnel may also examine workstation activity.

Intrusion detection tools will be used to monitor the Department networks, and the intrusion detection logs must be routinely reviewed. The Department must manage auditing trails and logs for monitoring, detecting attempted attacks, and allowing backtracking to the source of attacks, in accordance with the Department's Information Technology Security Controls Reference Guide.

#### 5.4.3. Network Security Architecture

The OCIO in coordination with the Program Offices shall establish and maintain a network architecture that includes security for both network components and connected IT systems. The Department must establish baseline security requirements in compliance with Federal guidelines as supplied in NIST SP's 800-12, 800-14, 800-18, 800-26, and 800-53.

Safeguards to complement the baseline security requirements shall be implemented to protect information resources, including the network's equipment, against misuse or attack to a level commensurate with their criticality or sensitivity. Network operational security controls shall be maintained commensurate with the approved acceptable level of risk.

A security perimeter must be established between the Department networks and external networks, including other Departments and Federal agencies, if appropriate. Services allowed to cross the perimeter must be controlled and restricted to specific resources.

#### 5.4.4. Network Connectivity

All external connections from the physical and network perimeters must be documented and secured in keeping with overall Department information systems security policies.

Prior to initiating such a connection, system security officers/system managers must demonstrate that there is a business need, that the approved security requirements have been met, that the accessing system does not compromise the existing security of the network or host the Department system, and that the accessing system complies with the Department standards. A connection to an external system must

have a sensitivity and criticality designation, and may have to submit to certification and accreditation, if the system meets the Department's requirements.

The Department must establish controls and obtain written management authorization (an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA)) for system interconnection. These agreements must be kept on file for reference. See NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, for guidance and samples on developing an ISA and a MOU/MOA. If the Department systems interconnect, they shall connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system. Where connection is authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.

The Department shall establish standards and guidance for the proper use of firewall, router, or gateway devices on the Department networks.

#### 5.4.5. Warning Banners

Department computers and IT systems must display a sign-on warning banner at all log-on points, where technically practical. The warning banner will be in accordance with the guidance set forth in the Information Technology Security Controls Reference Guide.

Orientation and security training or awareness programs for employees must include notification for using sign-on warning banners on all Department IT systems.

At a minimum, warning banners must state that the use of the Department IT systems is subject to monitoring and is for limited personal use by Department personnel; all data contained on Department IT systems are property of the U.S. Government; and there can be no expectation of personal privacy on the Department IT systems.

#### 5.4.6. Security Testing

Security testing and evaluation of all GSSs and MAs shall occur in conjunction with necessary certification and accreditation activities. Procedures and test plans shall be updated to reflect lessons learned and newly identified vulnerabilities.

Production data must not be used for testing purposes unless the data have been properly screened for sensitive material. Testing must incorporate and conform to all security and configuration management controls defined by the Department.

Testing results must be evaluated to ensure that an acceptable level of risk is maintained. IT systems security controls and activities must be adjusted accordingly. All testing and evaluation activities must be documented.

#### 5.4.7. Penetration Testing and Vulnerability Scans

Department GSSs and MAs containing mission-critical or sensitive data must undergo penetration testing and vulnerability scanning annually or as significant changes are made to the IT system(s). Where interconnected IT systems are present, analyses must be conducted frequently to identify security threats to the Department through shared system boundaries.

Prior to conducting penetration testing, rules of engagement must be developed and signed in coordination with all appropriate officials, which may include the SSO, CSO, and Director of IAS.

Penetration testing may identify previously unknown security problems, configuration errors, and needed patches or updates on mission-critical or sensitive IT systems. Vulnerabilities identified through penetration testing must be documented and passed on to the CSO and appropriate application managers for inclusion in POA&M's.

#### 5.4.8. Virus Protection

Department personnel and contractors must ensure that all reasonable measures are taken to prevent, detect, remove, and report malicious code (e.g., viruses, worms, and Trojan horses) from all IT systems and removable media.

The Director of ITOMS shall establish and implement procedures to minimize the risk of viruses on Department IT systems, detect and remove viruses from the Department IT systems.

Network administrators must ensure antivirus software is installed at the network perimeters and at any identified high-risk or sensitive gateways, and be deployed to workstations, file servers, e-mail servers, and Internet gateways to limit the spread of viruses within the networks.

Through Security Awareness Training, users must be informed about the procedures for detecting viruses and limiting the spread of infection.

Personnel must follow incident response procedures to report any unusual behavior that a computer or application exhibits or that malicious code has been detected.



## 6. APPENDIX A: GLOSSARY

**Accreditation:** The authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security.

**Authorize processing:** Activities that occur when management authorizes in writing a system based on an assessment of management, operation, and technical controls. By authorizing processing in a system, the management official accepts the risks associated with it.

**Certification:** The technical evaluation that established the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements.

**Critical Infrastructure Protection (CIP):** A description of how an organization intends to secure and safeguard its key assets both cyber and physical in support of the organizations essential operations.

**Designated Approving Authority (DAA):** The senior management official who has the authority to authorize processing (accredit) an automated information system (major application or general support system) and accept the risk associated with the system.

**Encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when it is stored on a transportable magnetic medium.

**Exhibit 53:** The agency's IT Investment portfolio to demonstrate the agency management of IT investments and how these governance processes are used to make decisions about IT investments within the agency.

**Exhibit 300:** A format for the Integrated Project Team to demonstrate to agency management and OMB that it has employed the disciplines of good project management, represented a strong business case for the investment, and met other Administration priorities to define the proposed cost, schedule, and performance goals for the investment if funding approval is obtained.

**Firewall:** A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

**General Support System (GSS):** An interconnected information resource under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, facilities, and people. It provides support for a variety of users or applications, or both.

**Interconnection:** The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

**Interconnection Security Agreement (ISA):** An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection.

**Least privilege:** The practice of granting users only those accesses they need to perform their official duties.

**Lifecycle Management (LCM):** The coordination of activities associated with the implementation of information systems from conception through disposal, which include defining requirements, designing, building, testing, implementing, and disposing of systems.

**Local area network (LAN):** A group of computers and other devices dispersed over a relatively limited area and connected by a communication link that enables a device to interact with any other on the network.

**Major Application (MA):** An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application.

**Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA):** A document established between two or more organizations to define their respective responsibilities in establishing, operating, and securing a system interconnection.

**Mission Essential Infrastructure (MEI):** The physical, cyber, data, and voice telecommunication facilities directly operated by the Department and on which the Department depends to carry out its critical missions.

**Network:** A system that includes communication capability that allows one user or system to connect to another user or system and that can be part of a system or a separate system. Examples of networks include LANs or WANs, including public networks such as the Internet.

**Password:** A confidential character string used to authenticate an identity or prevent unauthorized access.

**Personal electronic devices (PEDs):** A PC that can be carried for convenience and travel purposes. Portable systems are compact desktop computers that can have comparable processing, memory, and disk storage to desktop computers or limited processing memory and disk storage. Portable systems can connect with other networked devices, applications, and the Internet through various mechanisms, such as dial-up lines. Examples of PED's include Palm™ computing devices, Pocket PC™, Windows CE™ Handheld, Blackberry™, cell phones with information storage and processing capabilities, and intelligent pagers with storage and processing functions.

**Remote Access:** The process of communicating with a computer located in another place over a communication link.

**Risk:** The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

**Risk management:** The ongoing process of assessing the risk to automated information resources and information, as part of a risk-based 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.

**Rules of behavior:** Rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system.

**Security level designations:** The security level designation is a rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse) and the operational criticality of data processing capabilities (i.e., the consequences if data processing capabilities were interrupted for some period or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an automated information system is assigned for the overall security level designation.

**Sensitive data:** Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

**Sensitive information:** Any information of which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act). Yet this information would not have been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.

**Sensitive But Unclassified (SBU):** A category of information managed by ED that is not considered vital to the national security, but the indiscriminant disclosure of which would result in data/information degradation or loss of public confidence. This type of information is intended for use within the Department of Education, and in some cases within affiliated organizations, such as ED business partners. This information may be found to contain the label "For Official Use Only" or "For Internal Use Only" or "Privacy Act" Protected information, but it is still considered SBU. Disclosure of this information to unauthorized individuals may be against laws and regulations, or its disclosure may have negative ramifications for the Department of Education, its customers, or its business partners. Due diligence is required to protect this category of information.

**Separation of duties:** The practice of dividing roles and responsibilities so that a single individual cannot subvert a critical process.

**Significant change:** Examples of significant changes to an information system that should be reviewed for possible reaccreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

**Smart card:** A plastic card about the size of a credit card that can be used to store personal identification to authenticate an individual's identity.

**System security plan:** A plan that provides an overview of the security requirements of systems and describes the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behaviors of all individuals who access the system.

**Threat:** An activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

**Token:** Something that the user possesses and controls (typically a cryptographic key or password) used to authenticate the user's identity.

**Unclassified:** A category of information that is approved for public release. Disclosure of this information, whether authorized or unauthorized, will not have negative ramifications for the Department of Education, its customers, or its business partners.

**User:** Any 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 but normally does not report to either the manager or director of the facility or to an immediate supervisor who is the same for all users.

**Virus:** A program that infects computer files (usually other executable programs) by inserting copies of itself in those files. This infection is usually done in such a manner that the copies will be executed when the file is loaded into memory, allowing them to infect still other files, and so on. Viruses often have damaging side effects, sometimes intentionally, sometimes not.

**Vulnerability:** A flaw or weakness that may allow harm to occur to an IT system or activity.

**Wide area network (WAN):** A communications network that connects geographically separated areas.

## 7. APPENDIX B: ACRONYMS

BTA	Business Technology Advisor
C&A	Certification and Accreditation
CAP	Corrective Action Plan
CCID	Computer Crimes and Investigation Division
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CSO	Computer Security Officer
DAA	Designated Approving Authority
Department	U. S. Department of Education
DRP	Disaster Recovery Plan
ED	U.S. Department of Education
EDCIRC	ED Computer Incident Response Capability
EDNet	Department of Education's Network
EO	Executive Order
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISCAM	Federal Information System Controls Audit Manual
FOIA	Freedom of Information Act
GISRA	Government Information Security Reform Act
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GSS	General Support System
IA	Information Assurance
IAS	Information Assurance Services
I&A	Identification and Authentication
IAPMP	Information Assurance Program Management Plan
ISA	Interconnectivity Security Agreement
IT	Information Technology
ITOMS	Information Technology Operations and Maintenance Services
LAN	Local Area Network
LCM	Lifecycle Management
MA	Major Application
MEI	Mission Essential Infrastructure
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NDA	Nondisclosure Agreement
NIST	National Institute of Standards and Technology
NSO	Network Security Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OM	Office of Management
OMB	Office of Management and Budget
OPM	Office of Personnel Management
POA&M	Plan of Action and Milestone
PED	Portable Electronic Device
P.L.	Public Law
RIMS	Regulatory and Information Management Services
SBU	Sensitive But Unclassified
SP	Special Publication
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network

## 8. APPENDIX C: REFERENCES

### IA-related Laws and Government-wide Directives

Federal laws and executive directives are the authoritative basis for this Handbook for Information Assurance Security Policy. Statutory requirements establish minimum standards that agencies must meet to protect the privacy of personal information or sensitive government information resident in their agencies and to improve the productivity, efficiency, and effectiveness of Federal programs through the improved acquisition, use, and disposal of IT resources. The statutory and executive directive requirements that Department policies in this manual reflect include Public Laws (<http://uscode.house.gov/>), Executive Orders, NIST guidance, and other documents.

#### ❖ Federal Laws and Regulations:

- Computer Security Act of 1987, P.L. 100-235, as amended by P.L. 104-106
- E-Government Act of 2002 including Title III Federal Information Security Management Act (FISMA), P.L. 107-347
- Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001
- Freedom of Information Act (FOIA), 5 U.S.C. § 552
- Government Paperwork Elimination Act (GPEA), P.L. 105-277
- Government Performance and Results Act (GPRA), P.L. 103-62
- Homeland Security Presidential Directive/HSPD-7, December 17, 2003
- Information Assurance Act, P.L. 104-106 (Clinger-Cohen Act)
- Privacy Act of 1974, 5 U.S.C. § 552a

#### ❖ National Institute of Standards and Technology (NIST) Special Publications (SP) 800 Series:

- NIST SP 800-12, Introduction to Computer Security: The NIST Handbook, April 1997
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-based Model, April 1998
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006
- NIST SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000
- NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001
- Draft NIST SP 800-26, Revision 1, Guide for Information Security Program Assessments and System Reporting Form, August 2005
- NIST SP 800-30, Risk Management Guide for Information Technology Systems, January 2002
- NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002
- NIST SP 800-37, Guide for the Certification and Accreditation of Federal Information Systems, May 2004
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002
- NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002
- NIST SP 500-53, Recommended Security Controls for Federal Information Systems, February 2005

- Draft NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 15, 2005
  - NIST SP 800-60, Guide for Mapping Type of Information and Information Systems to Security Categories, June 2004
  - NIST SP 800-61, Computer Security Incident Handling Guide, January 2004
  - NIST SP 800-63, Electronic Authentication Guideline, September 2004
  - NIST SP 800-64, Revision 1, Security Considerations in the Information System Development Life Cycle, June 2004
  - NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process, January 2005
- ❖ **NIST Federal Information Processing Standards (FIPS) Publication:**
- FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
  - FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
  - FIPS Pub 201, Personal Identity Verification for Federal Employees and Contractors, March 2006
- ❖ **Office of Management and Budget (OMB) Circular:**
- OMB A-130, Management of Federal Information Resources, November 2000
    - OMB A-130, Appendix III, Security of Federal Automated Information Resources
  - OMB A-11, Preparation, Submission, Execution of the Budget, 2004
- ❖ **U.S. Government Accountability Office (GAO):**
- GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999

## Department IA-related Guides and Plans

The Chief Information Officer (CIO) issues guidance to advise Principal Offices on proper implementation of the IA security program. Listed below are the Department guidance and plans that implement and support the Department IA security program. Department documents are available on *connectED* site for OCIO/IAS.

- [Baseline Security Requirements](#)
- [Critical Infrastructure Protection Plan](#)
  
- Handbook OCIO-05, [Handbook for Information Technology Security Certification and Accreditation Procedures](#)
- Handbook OCIO-07, [Handbook for Information Technology Risk Assessment Procedures](#)
- Handbook OCIO-09, [Handbook for General Support Systems and Major Applications Inventory Procedures](#)
- Handbook OCIO-10, [Handbook for Information Technology Contingency Planning Procedures](#)
- Handbook OCIO-11, [Handbook for Information Technology Configuration Management Planning Procedures](#)
- Handbook OCIO-13, [Handbook for Telecommunications](#)
- Handbook OCIO-14, [Handbook for Information Security Incident Response and Reporting Procedures](#)
  
- Handbook OIG-1, [Handbook for Personnel Security-Suitability Program](#)
  
- [Information Technology Security Communications Guide](#)
- [Information Technology Security Compliance Guide](#)
- [Information Technology Security Cost Estimation Guide](#)
- [Information Assurance Program Management Plan \(IAPMP\)](#)
- [Information Technology Security System Development Life Cycle Integration Guide](#)
- [Information Technology Security Test & Evaluation Guide](#)
- [Information Technology Security Controls Reference Guide](#)
- [IT Security Metrics Program Plan](#)
  
- OCIO: 1-104, [Personal Use of Government Equipment](#)
  
- OM: 2-104, [Occupant Emergency Organizations and Plans](#)
- OM: 3-104, [Clearance of Personnel for Separation or Transfer](#)
- OM: 4-114, [Physical Security Program](#)
- OM: 5-101, [Contractor Employee Personnel Security Screenings](#)
- OM: 5-102, [Continuity of Operations \(COOP\) Program](#)
- Handbook OM-01, [Handbook for Classified National Security Information](#)
  
- EDNet-POL-000-0128, [Use of Laptop Equipment on EDNet](#)
  
- PMI 368-1 – [Flexiplace Program](#)