ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL HANDBOOK

Distribution:
All Department of Education Employees

Approved by: _____/s/_____
Michell C. Clark, Assistant Secretary
Office of Management

Handbook for Protection of Sensitive But Unclassified Information

For technical questions regarding this document, please contact Kathy Zheng via e-mail or on 202-245-6447.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

This directive sets forth requirements for protecting and securing the Department of Education (Department's) sensitive but unclassified information in order to ensure the confidentiality, integrity, and availability of agency information and information systems. The purpose of this document is to provide all personnel, including employees and support contractors with information necessary to protect sensitive but unclassified information from misuse, loss, or unauthorized disclosure. This document includes minimum protection requirements and recommends additional security safeguards to be applied where warranted by the sensitivity of the information.

1.2 Background

In response to numerous incidents involving the compromise or loss of sensitive personal information, OMB issued Memorandum M-06-16 to provide Federal agencies guidance on the protection of personally identifiable information entrusted to them.

The Department collects and maintains many types of sensitive but unclassified information and includes, but is not limited to, information related to the privacy of individuals, payroll and financial transactions, and proprietary information. It is essential that this information be properly handled, stored and protected from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction. One of the Department's primary responsibilities is to assure the security of the sensitive information it collects, produces, and disseminates in the course of conducting its operations.

1.3 Sensitive But Unclassified Information

Sensitive but unclassified information is information that is not classified for national security reasons, but that warrants/requires administrative control and protection from public or other unauthorized disclosure. Information, in either hard copy or electronic form, determined to be sensitive but unclassified information should meet one or more of the criteria for exemption from public disclosure under the Freedom of Information Act (FOIA), or should be protected by the Privacy Act, U.S.C. 552a. The exact language of the exemptions can be found in FOIA (5 U.S.C. 552).

Sensitive but unclassified information consists of any information exempted from FOIA and includes, but is not limited to, information related to personal, proprietary information, operations security protected information, and records or information compiled for law enforcement purposes. Examples include, but are not limited to:

- **Personally Identifiable Information (PII)** any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history **and** information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. PII that, if

improperly disclosed, could be used to steal an individual's identify, violate the individual's right to privacy, or otherwise harm the individual.

- **Proprietary** information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.
- **Security** information concerning functions, operations, programs, or any other information considered a security risk, such as, but not limited to, facility blueprints and other detailed facility information, databases associated with the physical security system, vulnerabilities of such facilities or sensitive information, network security information, security procedures, security audit results, incident reports and actions, and security plans.

Sensitive but unclassified information is intended for use within the Department, and in some cases within affiliated organizations. This type of 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 sensitive but unclassified. Disclosure of this information to unauthorized individuals may be against laws and regulations, or its disclosure may have negative ramifications for the Department, its customers, or its business partners. Due diligence is required to protect this category of information.

This directive is **not** meant to be interpreted as applicable to classified national security information as defined under Executive Order 12958, as amended. Departmental Handbook OM-01, *Classified National Security Information*, sets forth the security standards and safeguards to ensure protection of classified national security information (known as "classified information").

1.4 Applicability and Scope

All Department personnel, including government employees and support contractors, have a duty to protect the Department's sensitive but unclassified information from improper disclosure; and personnel with actual custody of sensitive but unclassified information record(s) are responsible for taking reasonable steps to safeguard them and are under an affirmative duty to report any known security breaches. Principal Offices may further supplement this policy with additional guidance in order to enforce more restrictive standards as appropriate. Principal Offices should identify and categorize their types of sensitive but unclassified information to include all FOIA exempt categories, and instruct employees and support contractors on proper protection of sensitive data.

1.5 Authorities

- 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
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources

- The Privacy Act of 1974, 5 U.S.C. § 552a
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 1, Recommended Security Controls for Federal Information Systems.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information
- The Freedom of Information Act (FOIA), 5 U.S.C. § 552, Amended in 2002

1.6 Compliance

It is the policy of the Department to safeguard sensitive but unclassified information within its control. The gross negligence or willful disclosure of sensitive but unclassified information may result in disciplinary action, including but not limited to, removal from employment. Violations of this policy may also result in civil and criminal penalties, including fines and imprisonment, under the laws of the U.S.

1.7 Exceptions

If compliance with any procedure 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. Exemption decisions shall be made between the Information Owner and/or System Owner/Manager and the Designated Approving Authority (DAA), in coordination with the CIO and/or the Chief Information Security Officer.

2. ROLES AND RESPONSIBILITIES

The roles and responsibilities described in this section are assigned to the positions identified to ensure effective protection of sensitive but unclassified information. All Department personnel, including employees and support contractors, who are responsible for, or associated with, the collection, creation, storage, use, transmission, handling, and/or dissemination of sensitive unclassified information share responsibility for its protection.

2.1 Chief Information Officer

The Chief Information Officer (CIO) provides advice and other assistance to the Secretary and other senior officers to ensure that information technology (IT) is acquired and information resources are managed for the Department in a manner that is consistent with the requirements of the Clinger-Cohen Act of 1996, the Federal Information Security Management Act of 2002 (FISMA), and industry best practices. In accordance with FISMA and the Clinger-Cohen Act, the CIO must

- Designate in writing a senior agency information security officer to execute the Department's IT Security Program;
- Develop and maintain information security policies, procedures, and control techniques to address all applicable requirements;
- Develop, maintain, and facilitate the implementation of a sound and integrated IT architecture for the Department;
- Promote the effective and efficient design and operation of all major information resources processes for the Department;
- Assist in the development of standards, guidelines, and policies to transform current Departmental data collection and information management processes;
- Train and oversee personnel with significant responsibilities for information security;
- With the support of the Chief Information Security Officer, work closely with authorizing officials and their designated representatives to ensure that the Department-wide security program is effectively implemented, that the certifications and accreditations required across the Department are accomplished in a timely and cost-effective manner, and that there is centralized reporting of all security-related activities; and
- Provide administrative and technical support to the agency's Data Integrity Board and monitor the Department's compliance with the Computer Matching and Privacy Protection Act.

2.2 Chief Information Security Officer

The Chief Information Security Officer (CISO) carries out the function of the senior agency information security officer as defined by FISMA. In this capacity, the CISO must coordinate with the CIO and

- Develop, document, and implement an agency-wide IT security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes--
    - Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption of information and information systems that support the operations and assets of the agency;
    - Policies and procedures for the Department's systems, to include developing related standards to be followed by all Principal and Staff Offices, and developing standards and practices to establish the Department's IT Security Program;
    - Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
    - IT security awareness training to inform personnel, including support contractors and other users of information systems that support the operations and assets of the agency;
    - Periodic security tests and evaluations of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually;
    - A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
    - Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines; and
    - Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the Department.
- Ensure IT security is included in the Department Strategic IT Planning and Enterprise Architecture efforts;
- Report to the Department's CIO and external entities, such as OMB and Congress, on the IT Security Program's status within the Department;
- Provide IT security guidance and technical assistance to all Principal and Staff Offices;
- Track Principal Offices weaknesses reported under self-assessments and external reviews and track implementation of corrective actions;
- Maintain a database of Principal Offices IT system inventories;
- Work cooperatively with the Department's Office of Inspector General, the Principal Offices, and other entities to ensure an effective IT Security Program;
- Promote and coordinate the Department-wide IT Security Program activities; and
- Identify resource requirements, including funds, personnel, and contractors, needed to manage the Department's IT Security Program.

2.3 Assistant Secretary for Management

The Assistant Secretary for Management (ASM) is the Department's senior agency official for privacy, and has overall responsibility and accountability for ensuring the Department's implementation of information privacy protections, including the agency's full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act, E-Government Act of 2002, and OMB guidance. In this capacity, the ASM shall:

- Approve new and altered Privacy Act System of Records notices for submission to OMB and Congress and publication in the *Federal Register*;
- Decide all written appeals of refusals to correct or amend records covered by the Privacy Act, as the Department's Privacy Appeals Officer;
- Approve regulations and directives regarding Privacy Act administration.
- Oversee, coordinate and facilitate the Department's information privacy compliance activities;
- Review the Department's information privacy procedures to ensure that they are comprehensive and up-to-date;
- Provide appropriate training and education programs on privacy laws, regulations, policies, and procedures governing the handling of personally identifiable information to the Department's employees and support contractors;
- Identify ways in which the agency can use technology to reinforce and sustain the privacy of personally identifiable information;
- Serve in a central role in evaluating the ramifications for privacy of legislation, regulatory and other policy proposals, as well as testimony and comments under OMB Circular No. A-19; and
- Participate in assessing the impact of technology on the privacy of personally identifiable information and identify ways in which the agency can use technology to reinforce and sustain the privacy of personally identifiable information.

2.4 Director, Office of Management (OM) Regulatory Information Management Services (RIMS)

The Director, OM/RIMS, serves as the Department's Privacy Officer and is responsible for managing the Department's Privacy Act Program. In this capacity, the Privacy Officer or designee has the following responsibilities:

- Review new and altered Privacy Act System Notices and System Reports for Assistant Secretary for Management approval, submission to OMB and Congress, and publication in the *Federal Register*;
- Review all Privacy Impact Assessments (PIAs) to ensure that they meet the requirements of Section 208 of the E-Government Act of 2002, approve the PIA documentation, and

make it publicly available, either in the *Federal Register* notice or on the Department's Web site (*www.ed.gov*);

- Review regulations and directives regarding Privacy Act administration;
- Establish a program to periodically review record-keeping policies and practices within the Department, in compliance with the Privacy Act;
- Consult with the Office of the General Counsel (OGC) on all legal matters related to implementation of the Privacy Act within the Department;
- Develop procedures and documents required to implement the Privacy Act, including reporting formats, directives, reports, and handbooks, in compliance with the Privacy Act, the Department's regulations, and OMB Guidelines;
- Provide technical assistance to system and program managers, as needed, in the development of the documentation required for System Notices, System Reports, Privacy Act statements, and PIAs;
- Ensure that the rules governing employee conduct, training and implementation of the Privacy Act requirements are current and sufficient;
- Coordinate the preparation of an annual report to OMB on compliance with Section 208 of the E-Government Act of 2002 (Public Law 107-347 44, U.S.C. Ch. 36); and
- Prior to consideration of all computer-matching agreements by the Department's Data Integrity Board, review all the agreements for computer matching programs under 5 U.S.C. § 552a(o) to ensure compliance with Departmental policies, OMB guidelines, and the Computer Matching and Privacy Protection Act of 1988.

2.5 Principal Officer

The Principal Officer is the senior individual administratively and operationally responsible for all information and information systems within the Principal Office or major component. The Principal Officer has centralized responsibility for the establishment, maintenance, and enforcement of the information security program and policy for all information and supporting systems within the Principal Office or business component. In this capacity, the Principal Officer shall:

- Consult with the OCIO, OM/RIMS, and OGC to ensure the proper use and handling of sensitive information; and
- Ensure that the Principal Office comply with the provisions of this directive.

2.6 Computer Security Officer

The Computer Security Officer (CSO) is the individual formally designated by a Principal Officer to be responsible for the implementation and management of the security policy within the organization. The CSO serves as the primary point of contact and coordination within the Principal Office for IT security matters. In this capacity, the CSO must

- Serve as a liaison between the Department's CISO and the Principal Office personnel responsible for IT security activities;
- Support management to assist them with the required IT security planning and budgeting for the Principal Office;
- Ensure that system users in, and support contractors for, the Principal Office receive the requisite security awareness training, as described in the Department's Information Technology Security Awareness and Training Program Plan;
- Ensure that employees and support contractors of the Principal Office are aware of their responsibility to protect sensitive information;
- Monitor and evaluate the security posture of all systems within the Principal Office;
- Ensure certification and accreditation of all systems under his/her responsibility including informing key officials of the need to conduct a security certification and accreditation;
- Ensure the performance of a risk analysis for each information system installation and resource within the Principal Office, as described in the Departmental *Handbook for Information Technology Security Risk Assessment Procedures*[1], and NIST SP 800-30, *Risk Management Guide for Information Technology Systems*; and
- Report and respond to IT security incidents, in accordance with the Departmental *Handbook for Information Security Incident Response and Reporting Procedures*[2].

2.7 Information Owner and System Owner/System Manager

The Information Owner is responsible for establishing the rules for appropriate use and protection of the subject information and retains that responsibility even when the information is shared with other organizations. The owner of the information stored within, processed by, or transmitted by an information system may or may not be the same as the system owner/manager. Information owners should provide input to information system owners regarding the security requirements and security controls for the information systems where the information resides. The information owner and the system owner/manager should work together to identify and categorize the information system and the information processed, stored, or transmitted by the system in accordance with the Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and document the results in the system security plan.

The System Owner/Manager is responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system, and may rely on the assistance and advice of the system security personnel in the implementation of the following security responsibilities. The system owner must

- Maintain active senior-level involvement throughout the development of the system;

[1] *Handbook OCIO-07*

[2] *Handbook OCIO-14*

- Determine and implement an appropriate level of security commensurate with the system impact level;
- Participate in project review activities and review project deliverables;
- Ensure the system is operated according to the agreed upon security requirements;
- Ensure that adequate security measures and procedures are implemented to protect the data residing on their system(s);
- Establish appropriate rules of behavior for all systems that apply to all personnel managing, administering, or having access to the system;
- Coordinate activities with the senior IT executive; and
- Hold review and approval authority for ensuring that developed products incorporate security and meet user requirements.

2.8 System Security Officer

The System Security Officer (SSO) is responsible for ensuring the appropriate security posture is maintained for the assigned system(s) or program. The SSO must

- Assist in the determination of an appropriate level of security commensurate with FIPS 199 and FIPS 200 security category of the system;
- Ensure that adequate management, operational, and technical security controls are implemented and maintained on the system, and that these controls are tested regularly;
- Assist in the development and maintenance of system security plans for all systems under their responsibility;
- Perform annual security assessment of the security posture of the system and reporting the status to the CSO;
- Participate in certification and accreditation of the system, ensure that appropriate resources are available for the effort, and provide the necessary system-related documentation to the OCIO/Information Assurance Services;
- Manage and control changes to the system and assess the security impact of those changes;
- Designate the user profiles, decide who has access to the information system and with what types of privileges or access rights;
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis; and
- Notify the CSO or the Education's Computer Security Incident Response Capability (EDCIRC) Coordinator of any suspected incidents in a timely manner.

2.9 Users

End user's responsibilities center upon being aware of the proper handling of sensitive information, as well as being vigilant in performing necessary security procedures in order to maintain the confidentiality and integrity of the information. All authorized users of the Department's information resources, including government employees and support contractors, either by direct or indirect connections, must

- Complete annual security awareness training;
- Know and abide by all applicable Departmental policies and acceptable uses as outlined in the Departmental *Handbook for Information Assurance Security Policy*;
- Exercise care and judgment to ensure adequate protection of the Department's sensitive information;
- Notify the appropriate Help Desk, SSO, CSO or the EDCIRC Coordinator of any suspected incidents in a timely manner; and
- If the user uses mobile devices to access the Department's information resources, the acceptable use guidelines outlined in the Departmental *Handbook for Information Assurance Security Policy* must be followed, including the requirements described in this document.

3. PROTECTION OF SENSITIVE INFORMATION

OMB Memorandum M-06-16 specifies measures that agencies need to have in place to ensure protection of sensitive information. To comply with OMB Memorandum M-06-16, the Department requires that Principal Office IT security programs include procedures for designating, marking, storing, handling, and destroying sensitive but unclassified information (both in hard copy and in electronic form) in accordance with NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*.

3.1 Access

The Department has been entrusted with sensitive information, including personally identifiable information, to accomplish its mission. This data must be protected from unauthorized disclosure, damage, fraud, and abuse. NIST 800-53 control MP-2 requires that only authorized users have access to information in printed form or on digital media removed from the information system.

The Department requires that all personnel be subject to an appropriate background check prior to permitting access to the Department's information resources. Appropriate background checks must be performed on the Department's employees and support contractors prior to their being given access to the Department's systems and networks in accordance with requirements contained in the Departmental *Handbook for Personnel Security – Suitability Program*[3], and the directive on *Contractor Employee Personnel Security Screenings*[4]. Sensitive information should only be accessed by authorized personnel who have a specific job-related need-to-know for that information. The responsibility for determining whether an individual has a need for access to sensitive information should be determined by the system owner/manager who has authorized possession, knowledge, or control of the information. In addition, the principles of separation of duties and least privilege must be applied to ensure that moderate- and high-impact systems enforce the most restrictive set of rights/privileges or accesses needed by individuals for the performance of specified tasks (NIST 800-53, AC-6).

- Systems that contain sensitive information must enforce assigned authorizations for controlling access to the system in accordance with applicable policy. For moderate- and high-impact systems, the system owner/manager must ensure that access to security functions and security-relevant information is restricted to authorized personnel (NIST800-53, AC-3).
- The process for granting users access through remote authentication should be periodically evaluated in accordance with OMB M-04-04, *E-Authentication Guidance for Federal Agencies* and NIST SP 800-63, *Electronic Authentication Guideline.*
- For high-impact systems, unless guard stations control access to media storage areas, the system owner/manager must employ automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.

[3] *Handbook OIG-01*

[4] *Directive OM:5-101*

- When sensitive information must be shared with support contractors and entities outside the Department, a Non-Disclosure Agreement Form must be executed by the responsible authority prior to granting access to the data.
- All Statements of Work (SOW) and Procurement Requests for IT services on systems that contain sensitive information must contain specific security requirements to include background investigations.

3.2 Identification and Marking

NIST 800-53 control MP-3 requires that the organization affix external labels to removable information system media (e.g., diskettes, external/removable hard drives, flash/thumb drives, compact disks) and information system output (e.g., paper printouts, hardcopy documents output from the information system) indicating the distribution limitations and handling caveats of the information. The Department requires that for high-impact information systems, Principal Offices must affix external labels to removable information storage media and printed output indicating the distribution limitations, handling caveats, and applicable security markings, if any, of the information. To provide for adequate handling of the agency's sensitive information, system owners/managers must ensure that all media containing sensitive information rated high are appropriately marked with the sensitivity of the information stored on the media. At a minimum, hardcopy documents and printouts containing sensitive information should have appropriate markings and labels. Labeling should include any special handling instructions. In addition, Principal Offices must document in their procedures specific types of media or hardware components exempt from labeling so long as they remain within a secure environment.

3.3 Storage

NIST 800-53 control MP-4 requires that the organization physically controls and securely stores moderate- and high-impact information systems media, both in hard copy and in electronic form, based on the highest FIPS 199 security category of the information recorded on the media. System owners/managers are required to categorize the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199, and documents the results in the system security plan.

To comply with OMB M-06-16 and NIST 800-53, the Department is implementing the following controls that both mandate and achieve encrypted storage of the information at the remote location:

- System owner/managers must establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage (NIST 800-53, PL-4). Users are required to sign an acknowledgement form indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.
- All sensitive information existing in hard copy should be stored within a locked container in a limited or exclusion area, an access controlled electronic environment, or be under the physical control of an authorized individual.

- Information that is considered sensitive by the originator and/or a system owner/manager, or determined to have a high value, or information that represents a high risk must be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage (NIST 800-53, SC-8 & 9).
- When cryptography is employed within the information system, system owners/managers must ensure that information systems perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation (NIST 800-53, SC-13).
- Employees whose work requires access to the Department's sensitive information, including personally identifiable information, will be allowed to download to remote or mobile devices only when required by official duties; this information must be encrypted during storage to protect against unauthorized disclosure. When the information is no longer required for a permitted purpose, it must be deleted within 90 days of last use as mandated by OMB M-06-16. The Department has actively pursued the encryption of data on mobile computers and devices. The Department is in the process of purchasing encrypted flash drives and mobile device hard disk and file encryption software to address the requirement for encrypting all data.
- All sensitive information must be encrypted when stored on mobile or remote commuters/devices.

3.4 Transmission

NIST 800-53 control MP-5 requires that the organization protects and controls information system media, both digital and non-digital media, during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. To address the requirements, the Department requires Principal Offices to develop and implement procedures that govern the movement of information system media include both digital and non-digital media. The receipt and delivery of such media should be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit. System owners/managers must control moderate- and high-impact systems media and restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel. In addition, the Department is developing and implementing procedures to ensure that transported media containing sensitive information will be encrypted.

OMB M-06-16 recommends encryption for agency sensitive information being transported and/or stored off-site. The Department is in the process of evaluating an off-site data encryption solution to address this issue. NIST 800-53 controls SC-8 and SC-9 require agencies employ cryptographic mechanisms to prevent unauthorized disclosure of information and to ensure recognition of changes to information during transmission unless protected by alternative physical measures.

- Sensitive information should be encrypted and authenticated if it is transported outside of the Department's network. User authentication or identification must be coupled with the encryption and data transmission processes to be certain that sensitive data is delivered only to authorized parties.

- Sensitive but unclassified information may be transmitted via e-mail to and from the Department e-mail addresses ([…]@ed.gov) that reside completely within the Department's network; but the sensitivity of some information may require a higher level of protection. The level of protection should be commensurate with the FIPS 199 security categorization of the information. Information that: (1) has been determined by the originator and/or an information owner/system owner to have a high value, (2) represents a high risk to the Department in the event of an unauthorized disclosure or undetected modification, or (3) has been categorized to have a FIPS 199 impact level of moderate or high, then such information must be encrypted or in a password-protected attachment if it is communicated via e-mail to internal and external users. The password must be strong and provided to the recipient under separate cover. Passwords must meet the requirements set forth in the Departmental *Handbook for Information Assurance Security Policy*[5].

- Personally identifiable information (information can be used to distinguish or trace an individual's identity, such as social security number, date and place of birth, or mother's maiden name) should not be communicated via e-mail, unless it is encrypted or in a password-protected attachment. With respect to any other information protected by the Privacy Act, users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to hardcopy documents. If there is any doubt as to how specific sensitive information ought to be handled, the matter should be brought to the attention of the appropriate supervisor or the holder of the information for clarification.

- Systems that contain sensitive information will be allowed for remote access only after an explicit request is made and approved by the Principal Office IT Coordinators or authorized by the Department management. Access must be permitted through a centrally managed virtual private network (VPN) that provides encryption and secure authentication.

- The process for granting users access through remote authentication should be periodically evaluated in accordance with OMB M-04-04, *E-Authentication Guidance for Federal Agencies* and NIST SP 800-63, *Electronic Authentication Guideline.*

- Employees in possession of sensitive information outside of controlled areas must take adequate precautions that afford positive accountability of the information and to protect such information from unauthorized access. In addition, employees whose work involves manipulating large quantities of sensitive information at home must obtain appropriate authorization from the responsible authority and comply with Departmental policies and procedures in taking this information home and properly protecting it.

3.5 Media Sanitization and Disposal

OMB M-06-16 mandates that any files containing sensitive information must be destroyed within 90 days when they are no longer required for a permitted purpose. In addition, NIST 800-53 control MP-6 requires that the organization sanitizes or destroys system media, both digital and non-digital, before its disposal or release for reuse outside the organization, to prevent

[5] *Handbook OCIO-01*

unauthorized individuals from gaining access to and using the information contained on the media. To comply with OMB M-06-16 and NIST 800-53, the Department is incorporating the following practices into the Departmental procedures for common controls or system security plans for system-specific controls, as appropriate:

- Personnel are not authorized to retain sensitive unclassified information permanently and must delete it within 90 days of last use when no longer required to carry out their work or project.
- All contracts and agreements for work that require or may require access to, or custody of, sensitive information must specify that at the conclusion of work the persons must return to the Department all sensitive information that was obtained or prepared as the result of work under the contract or agreement.
- Hard copy media must be destroyed by shredding, pulping or any other accepted method to assure destruction beyond recognition and reconstruction. It is acceptable to dispose of sensitive but unclassified information in containers that are designed to accept it and where it will be disposed of properly under controlled conditions.
- Electronic media must be destroyed in accordance with NIST 800-88, *Guidelines for Media Sanitization*. Electronic media (e.g., diskettes, removable hard drives, flash/thumb drives, USB drives) may be recycled for use only with information of the same or higher sensitivity.
- Before any media are sanitized, system owners/managers must ensure that historical information is captured and maintained where required by business needs. Documentation (electronic or hard copy) qualifying as Federal records must be archived in accordance with the Departmental *Records and Information Management Program*, and the National Archives and Records Administration.

3.6 Security Awareness Training

FISMA requires Federal agencies to provide mandatory periodic training in computer security awareness and accepted security practice of all personnel who manage, use, or operate a Federal information system. The Department requires mandatory periodic security awareness training to be incorporated into its training programs to communicate responsibilities and disciplinary processes regarding the appropriate use of the Department's information and information systems. All personnel including employees and support contractors, who are authorized access to the Department's information and information systems must undergo periodic security awareness training.

3.7 Incident Reporting

FISMA requires all agencies to report security incidents to the U.S. Computer Emergency Readiness Team (US-CERT) within the Department of Homeland Security.

- As required by OMB M-06-19, all incidents involving personally identifiable information must be reported to US-CERT within one hour of discovering the incident by the EDCIRC Coordinator or designee.
- When reporting incidents as possibly involving personally identifiable information, there must be sufficient reason to believe that a security breach has occurred and that personally identifiable information is likely to have been involved. Otherwise, the incident must be reported to the appropriate Help Desk, or the relevant SSO, CSO or the EDCIRC Coordinator in accordance with the Departmental *Handbook for Information Security Incident Response and Reporting Procedures*[6].
- Employees or support contractors who observe suspicious or inappropriate requests for information by any means (e.g., e-mail or verbal) must report them to the relevant CSO.

[6] *Handbook OCIO-14*

4. INFORMATION AND INFORMATION SYSTEM SECURITY

The OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, states that there is a "presumption that all [systems] contain some sensitive information." The Department is required by OMB Circular A-130 to protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information. System owners/managers must assess their security risks and take appropriate measures to protect the confidentiality and integrity of the information contained in their information systems and networks.

4.1 Information Assets

Information assets need to be suitably classified to ensure that they receive an appropriate level of protection commensurate with their sensitivity and criticality. System owners/managers must assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of information and information systems and implement security measures to reasonably mitigate such risks and vulnerabilities to an acceptable level.

4.1.1 Security Categorization

System owners/managers must categorize the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199, and document the results in the system security plan. System owners/managers and system security personnel must work together to ensure that appropriate controls are in place and functioning to provide an adequate level of security as required by OMB A-130. Once the security category for the system is determined, the owner/system manager must develop acceptable control baselines appropriate to the system's impact level in accordance with NIST 800-53.

4.1.2 Privacy Impact Assessment

In accordance with FISMA and OMB, a privacy impact assessment (PIA) must be conducted for any system, program, or technology that involves personally identifiable information to ensure that information is handled in a manner that maximizes both privacy and security. The Department requires system owners/managers to comply with the requirements of the e-Government Act of 2002, Public Law 107-347, section 208, and associated guidance from OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, regarding privacy impact assessments.

4.1.3 Risk Assessment

Security and the need to protect sensitive information must be commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. System owners/managers must comply with NIST 800-53 controls for risk assessment of all Department's systems and applications under their responsibility. In addition, if the system uses electronic authentication methods to provide services, the risk

assessment must include an e-authentication risk assessment compliant with OMB M-04-04, *E-Authentication Guidance*, and associated implementation requirements in NIST 800-63, *Electronic Authentication Guideline*. System owners/managers are required to update risk assessments at least every three (3) years or whenever there is a significant change to the system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system as required by OMB A-130. The system owner/manager may acquire a third party to conduct the assessment, or use in-house personnel.

During the system risk assessment, the system owner/manager must determine the sensitivity of the agency's mission to compromises of confidentiality, integrity, and availability of the information stored and processed by the system. This determination, along with the likelihood of compromise occurring and the extent of protection required by law, establishes the level of security adequate to protect the data as required by OMB A-130, Appendix III. The system owner/manager then identifies the management, technical, and operational controls appropriate to provide the required protection.

4.1.4 Certification and Accreditation

Certification and accreditation (C&A) is the process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect information systems and data stored in and processed by those systems. The C&A process implements the concept of adequate security, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information, which is defined in OMB Circular A-130. NIST 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on security certification and accreditation of information systems.

System owners/managers must ensure that all Department information systems have been certified and accredited for operation in accordance with NIST 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and the Departmental *Handbook for Information Technology Security Certification and Accreditation Procedures*. All information systems require certification as a prerequisite to obtaining an accreditation decision. In addition, FISMA requires that agencies provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. That is, agency IT security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. System owners/managers must ensure that all contractor systems used to process, store, or transmit Department information are certified and accredited in accordance with C&A guidance. To ensure C&A activities can take place, system owners/managers, Contracting Officers, Contracting Officer's Technical Representatives, and others involved in aspects of system security must include specific language in contracts to ensure applicability of Department IT Security Program policies to all Department support contractors.

4.2 Data Repositories

Databases and applications that interface with databases, must be configured in accordance with security best practices:

- Table access controls must be applied to databases containing sensitive unclassified data. Access to specific data within the database will be limited to only those personnel who need access, and will be limited to only those functions (*e.g.*, read, modify) required for the person to perform his or her duties.
- Database servers must only allow connections from authorized, trusted sources (such as the specific web servers to which they supply information).
- For sensitive data, audit trails must be created and maintained within the database to track transactions and provide accountability. Audit logs must be retained for a reasonable period as documented in the system security plan and consistent with Departmental and National Archives and Records Administration retention periods, to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
- Database servers and database software must adhere to all Department information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.
- Sensitive information stored on the Department network must be protected at level that can ensure that only those who are authorized to view the information are allowed access (e.g., machine-generated passwords, encryption). The Department network systems must maintain a high level of electronic protection (e.g., firewalls, intrusion detection, defense-in-depth) to ensure the integrity of sensitive information and to prevent unauthorized access in these systems. Regular review of the protection methods used and system auditing are also critical to maintain protection of these systems.

4.3 System Interconnection/Information Sharing

NIST 800-53 requires that the organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis. A system interconnection is defined as the direct connection of two or more information systems for sharing data and other information resources. Before interconnecting their information systems, each organization must ensure that its respective system is properly certified and accredited in accordance with NIST C&A guidelines. Principal Offices must examine the sensitivity level of data or information resources that will be exchanged or passed over the interconnection and determine whether such use is restricted under current regulations or policies. Permission to exchange or transfer data must be documented, along with a commitment to protect such data. This information should be addressed in an Interconnection Security Agreement (ISA) and a Memorandum of Understanding or Agreement (MOU/A). If the interconnection is used to exchange or transfer sensitive data, system owners/managers must ensure that users understand special requirements for handling such data, if required. Principal

Offices should review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure the controls are operating properly and are providing appropriate levels of protection. The Department requires that system owners/managers utilize the methodology for documenting system support and interconnectivity agreements as developed in accordance with NIST 800-47, *Security Guide for Interconnecting Information Technology Systems*.

4.4 Remote Access

OMB M-06-16 recommends that agencies allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. The Department's OCIO provides employees with remote access connections to the Department's information resources. Appropriate officials must authorize each remote access method for the Department's information systems and authorize only the necessary users for each access method. Please consult the Remote Access Service Policy & Procedures for details on how to obtain permissions for VPN and Dial-in access. Authorized users can access the Department's sensitive data such as personally identifiable information remotely through a centrally managed VPN and dial-in service that provide secure authentication. The Department is leveraging the HSPD-12 requirement to enforce the use of two-factor authentication for remote access to the Department's information resources.

NIST SP 800-53 requires that the organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. All remote connections to the Department's information resources are subject to the same rules, policies, and practices just as if they were in the office. All remote access sessions will timeout after 30 minutes of inactivity and will require reconnection and authentication to re-enter the network in the manner described in the OMB M-06-16.

4.5 Mobile Security

The increased usage of mobile devices such as laptops, BlackBerrys, thumb drives and other mobile devices provides users with greater flexibility and efficiency in accomplishing the mission of the Department. However, as a consequence of the convenience and portability of these devices, their use creates additional challenges to maintaining the confidentiality and integrity of the Department's data. Increased effort and awareness is required to protect sensitive data on these types of systems. Many of the same basic principles governing the protection of data on desktop systems apply equally to portable systems. Mobile users must take reasonable steps to mitigate the vulnerabilities and risks associated with mobile computing:

- Never set the login dialog box to remember the password;
- Keep antivirus protection up-to-date, as well as the operating system and application security patches;
- Password-protect all devices, such as removable drives and compact disks (CDs),
- Do not store unencrypted sensitive information on mobile devices;

- Incorporate a time-out function that requires re-authentication after 30 minutes of inactivity;
- Back up your data to a location separately from the device;
- Include both hardware/device-based authorization and application-based authorization for access control mechanisms;
- Do not keep mobile devices online when not in use. Either shut them off or physically disconnect them from the Internet connection; and
- Lost or misplaced government-issued devices must be immediately reported to the Principal Office IT Coordinators (POCs) and/or the relevant CSO.

4.6 Laptop Security

Laptop computers offer the convenience of mobility, but the risk of lost or stolen machines and of wrongful access to the Department's sensitive data is high. The use of Department-owned laptops demands attention to security precautions. Every employee issued a Department-owned laptop is responsible for the security of that laptop and its data, regardless of whether the laptop is used in the office, at the employee's home, or in any other location such as an airport, hotel or car. Users must follow the following requirements:

- All laptops must be authorized by the relevant POC or the responsible authority.
- Any approved movement of laptops must be accompanied by an authorized hand receipt and hand receipts must be maintained on file for audit verification.

Laptops are a prime target for theft everywhere. So given the risk of laptop theft and the potential losses that laptop theft can cause, there are some security measures that individuals can take to protect the laptop and the information on it.

- Use a login password that is not easily guessed. The password must meet the requirements set forth in the Departmental *Handbook for Information Assurance Security Policy*.
- Never keep passwords or account numbers on the machine or in the case.
- Keep the laptop out of sight when not in use, preferably in a locked drawer or cabinet.
- Never let the laptop out of your sight in an airport or other public area.
- When traveling by plane or rail, never place the laptop in checked baggage.
- Never put the laptop on the conveyor belt at a security checkpoint until the person in front of you has successfully passed through the metal detector.
- Never leave the laptop visible in a vehicle. If you must, cover it with something or put it in the trunk.

- Avoid leaving the laptop in a hotel room, but if you must do so, use a cable lock or at least lower the risk of theft by keeping it out of sight. Locking it securely in another piece of luggage or room safe should make it secure from theft.
- Store all sensitive data files in encrypted form will prevent disclosure of the data even if the laptop is stolen.
- Keep only software files on the laptop's hard drive. Back up sensitive data to a location other than the laptop hard drive. Keep CDs and diskettes and carry them separately from the laptop.
- If the laptop is stolen or lost, it must be immediately reported to the relevant POC and/or your CSO.

APPENDIX A. GLOSSARY OF TERMS

Accreditation: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Availability: Ensuring timely and reliable access to, and use of, information and information systems.

Certification: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Controlled Area: Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Electronic media (or soft copy): Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types listed in NIST 800-88.

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.

Hard Copy Media (non-digital): Physical representations of information. Paper printouts, printer, and facsimile ribbons, drums, and platens are all examples of hard copy media.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

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

Interconnection Security Agreement (ISA): In this guide, an agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.

Media: Physical devices or writing surfaces including, but no limited to, magnetic tapes, optical disks, magnetic disks, and printouts onto which information is recorded, stored, or printed within an information system.

Media Sanitization: A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Memorandum of Understanding/Agreement (MOU/A): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

Need-to-Know: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Risk Assessment: The process of identifying risks to agency operations, agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

Sanitize: Process to remove information from media such that data recovery is not possible.

Sensitive But Unclassified Information: Information that may be exempt from mandatory release to the public under FOIA. Sensitive but unclassified information is the formal designation for information that by law or regulation requires some form of protection but is outside the formal system of classification, as in accordance with Executive Order 12958, as amended. Sensitive but unclassified information is intended for use within the Department, and in some cases within affiliated organizations. 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 sensitive but unclassified. Disclosure of this information to unauthorized individuals may be against laws and regulations, or its disclosure may have negative ramifications for the Department, its customers, or its business partners.

System of Records: Any group of records under the Department’s control from which information is retrieved by a personal identifier. Single records or groups of records that are not retrieved by a personal identifier are not part of a System of Records. Papers maintained by Department employees that are prepared, maintained, or discarded at the discretion of the employee and that are not subject to the Federal Records Act (44 U.S.C. § 2901), are not part of a System of Records--provided that such personal papers are not used by the employee or the Department to determine any rights, benefits, or privileges of individuals.

APPENDIX B. ACRONYMS

ASM	Assistant Secretary for Management
C&A	Certification and Accreditation
CD	Compact Disk
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Computer Security Officer
Department	Department of Education
EDCIRC	ED Computer Security Incident Response Capability
EDNet	Department of Education's Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ISA	Interconnection Security Agreement
IT	Information Technology
MOU/A	Memorandum of Understanding or Agreement
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OM	Office of Management
OMB	Office of Management and Budget
PDA	Personal Digital Assistant
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POC	Principal Office Coordinators
RAS	Remote Access Service
RIMS	Regulatory Information Management Services
SOW	Statements of Work
SSO	System Security Officer
USB	Universal Serial Bus
US-CERT	US Computer Emergency Response Team
VPN	Virtual Private Network

APPENDIX C. REFERENCES

Classified National Security Information	Executive Order 12958, as amended; ISOO Directive No. 1
Computer Security Act	Computer Security Act of 1987, P.L. 100-235, as amended by P.L. 104-106
FISMA	E-Government Act of 2002 including Title III Federal Information Security Management Act (FISMA), P.L. 107-347
OMB A-130	Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-130, Appendix III, November 28, 2000 (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

DEPARTMENTAL HANDBOOKS AND DIRECTIVES

OCIO-01, Handbook for Information Assurance Security Policy

OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures

OCIO-14, Handbook for Information Security Incident Response and Reporting Procedures

OM:6-103, Records and Information Management Program

OM:6-104, The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information)

Privacy Act of 1974, 5 U.S.C. § 552a

NIST STANDARDS AND GUIDELINES

NIST FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, February 2004 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)
FIPS Pub 200	Minimum Security Requirements for Federal Information and Information Systems, March 2006 (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf)
NIST SP 800-30	Risk Management Guide for Information Technology Systems, January 2002 (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
NIST SP 800-34	Contingency Planning Procedures for Information Technology Systems June 2002 (http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf)

NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004 (http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf)
NIST SP 800-47	Security Guide for Interconnecting Information Technology Systems August 2002 (http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf)
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program, October 2003 (http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf)
NIST SP 800-53 Revision 1	Recommended Security Controls for Federal Information Systems, December 2006 (http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf)
NIST SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, April 2006. (http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)
NIST 800-88	Guidelines for Media Sanitization, September 2006 (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)