

## Department of the Interior Departmental Manual

---

**Effective Date:** 3/21/12

**Series:** Information Resources Management

**Part 375:** IRM Program Management

**Chapter 19:** Information Security Program

**Originating Office:** Office of the Chief Information Officer

---

### 375 DM 19

**19.1 Purpose.** This chapter establishes the Department's information security program.

**19.2 Definitions.** Information security terms utilized in this chapter are defined in the National Institute of Standards and Technology (NIST) Internal Review 7298, *Glossary of Key Information Security Terms*.

**19.3 Scope.** This chapter applies to all employees and other users of Department of the Interior (DOI) information systems.

**19.4 Authorities.** Authorities for this chapter are listed in Appendix A. The chapter will be updated as necessary, such as when new laws concerning information security are enacted by Congress and/or new guidance is issued by the Office of Management and Budget (OMB) or NIST.

**19.5 Roles and Responsibilities of Department Personnel.** The roles and responsibilities of Department personnel with respect to information security are as follows:

A. **Chief Information Officer (CIO).** The CIO is the Department of the Interior (DOI) Information Technology Risk Executive and is responsible for:

(1) Ensuring DOI information system risk management processes are linked to DOI mission risk management processes at the Department level; and information system risks are viewed from an agency-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core mission and business functions.

(2) Designating the following Information Technology (IT) program officials:

(a) Chief Information Security Officer (CISO)

(b) Authorizing Officials (AOs) - (must be designated in writing)

3/21/12 #3941

Replaces 4/15/02 #3397

(3) Establishing department-wide information security policy, standards, and guidance; and overseeing implementation to ensure compliance for all information and information systems, as required by the Federal Information Security Management Act of 2002 (FISMA) and 112 DM 24.

B. Director, Office of Law Enforcement and Security. Responsible for obtaining accreditation from appropriate authorities for all national security systems processing classified information.

C. Heads of Bureaus and Offices. The Heads of bureaus and offices are responsible for ensuring compliance with applicable Federal laws, rules, regulations, policies, standards, and procedures including those issued by OMB, NIST and the Department for their mission/business operations, practices, information and information systems.

D. Chief Information Security Officer (CISO). Responsible as the Senior Agency Information Security Officer (SAISO) for developing and maintaining an agency-wide information security program, the CISO is also responsible for carrying out the CIO's information security responsibilities under Federal law and heading an office with the mission and resources to manage the overall Information Security Program

E. Employees and Volunteers. Responsible for complying with applicable Federal laws, rules, regulations, policies, standards and procedures including those issued by OMB, NIST and the Department to include, but not limited to, the following:

- (1) Properly using and protecting agency data, information and information systems ensuring their use is only for the execution of official duties or authorized purposes.
- (2) Promptly reporting potential security incidents and breaches.
- (3) Adhering to established Rules of Behavior.
- (4) Completing required training.

**19.6 Applicable Standards and Guidelines.** The standards, guidelines, and implementation plans provided in this section comprise the documentation necessary to effectively establish the information security program of the Department.

A. Information Security Standards and Guidelines Issued by the Office of the Chief Information Officer (OCIO). The OCIO shall issue the following information security standards and guidelines:

- (1) Information security standards based on the NIST information security control standards in the current version of Special Publication (SP) 800-53, that pertain to NIST defined 3/21/12 #3941  
Replaces 4/15/02 #3397

security categories or “control families” listed in the table in Appendix B.

(2) Information security standards specific to the needs of DOI.

(3) Information security guidelines governing the implementation of the standards referenced in sections 1 and 2 above for all IT infrastructure across the Department including all bureaus, offices and subordinate organizations.

(4) Security Technical Implementation Guides (STIGs) governing the technical implementation of the security standards referenced above.

B. Information Security Guidelines and Implementation Plans Issued by Bureaus and Offices. Bureaus and offices are responsible for issuing the following information security guidelines and implementation plans:

(1) System Owners shall issue detailed information security plans that must be approved by the Authorizing Official (AO) consistent with the OCIO standards and guidelines defined above.

(2) Assistant Directors for Information Resources with the concurrence of the DOI OCIO shall issue information security guidelines that define how information security standards should be implemented across a bureau or office for mission applications. These guidelines may provide additional security details for a particular bureau or office and its mission IT systems, but may not contradict existing OCIO standards or guidelines.

C. Risk Management Framework.

(1) The OCIO will issue an Information Security Risk Management Framework (RMF) consistent with all relevant NIST standards.

(2) The RMF will establish the Department’s strategy to mitigate information security risks associated with the operation and use of information systems and the implementation requirements of this strategy across the Department. Any residual information security risks will be explicitly accepted by the AO as part of the Assessment and Authorization (A&A) process for all Major Applications (MA) and General Support Systems (GSS).

(3) The NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* identifies additional roles and responsibilities required by the RMF.

**19.7 Compliance with Standards and Guidelines.** The OCIO will issue information security standards and guidelines in support of this chapter and work with Human Resources personnel, contracting officers and any other personnel needed to ensure compliance with such standards and guidelines throughout the Department. Bureaus and offices will issue guidelines and

3/21/12 #3941

Replaces 4/15/02 #3397

implementation plans, consistent with the OCIO standards and guidelines, and ensure compliance within their respective organizations of the OCIO standards and guidelines, as well as the bureau and office guidelines and implementation plans.

#### 19.8 **Classified National Security Systems**

A. The Chief of National Security Programs within the Office of Law Enforcement and Security maintains oversight for all classified network systems department-wide and is responsible for accesses and for obtaining accreditation of all national security systems processing classified information.

B. Systems within the Department that process Sensitive Compartmented Information (SCI) must meet the same security standards as systems that process controlled unclassified information.

C. In addition to the standards referenced in paragraph 19.8 B., systems processing collateral (non-SCI) national security information must comply with security policy established by the Committee on National Security Systems (CNSS).

D. In addition to the standards referenced in paragraph 19.8 B., systems processing SCI must comply with security policy established by the Director of National Intelligence (DNI) in Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*.

E. Bureaus and offices shall comply with DOI policies and directives regarding national security information and industrial security programs, ICD 503 and CNSS policies to manage the security of their National Security Systems and use NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, to identify National Security Systems.

## Appendix A Relevant Authorities

Applicable Laws. A number of laws, policy guidelines, regulations and guidance directives mandate protection of Federal computers, information, and related resources. Applicable laws passed by Congress include:

Authority	Description
Federal Records Act of 1950, 44 U.S.C. §§21, 29, 31 and 33	Establishes the framework used by Federal agencies for their Records Management programs.
The Freedom of Information Act (FOIA) of 1966, 5 U.S.C. § 552	Requires that Federal information be made available to the public except under certain specified conditions.
The Privacy Act of 1974, 5 U.S.C. § 552a	Imposes collection, maintenance, use, safeguard, and disposal requirements for Executive Branch offices maintaining information on individuals in a “system of records.”
Federal Managers Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. § 3512	Mandates that Federal agencies establish and maintain an internal control program to safeguard data processing resources, assure their accuracy and reliability, and protect the integrity of information resident on such systems.
Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030	Provides for the punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse government resources, and/or conduct fraud on government computers.
Government Performance and Results Act (GPRA) of 1993, 31 U.S.C. § 1101	Establishes policies for managing agency performance of mission, including performance of its practices.
Paperwork Reduction Act of 1995, Revised, 44 U.S.C. §§ 3501-3520	Provides for the administration and management of computer resources.
Clinger-Cohen Act – Information Technology Management Reform Act of 1996, 40 U.S.C. § 1401 <i>et seq.</i>	Improves the acquisition, use, and disposal of Information Technology (IT) by the Federal government.
Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3111	Mandates Federal agencies to implement and maintain financial management systems that comply substantially with Federal systems requirements, Federal accounting standards, and the U.S. Government Standard General Ledger (SGL). FFMIA also requires GAO to report annually on the implementation of the act.

Authority	Description
National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030	Provides for the protection of computer resources.
Government Paperwork Elimination Act (GPEA) of 1998, 44 U.S.C. § 3504	Provides for Federal agencies to give persons who are required to maintain, submit, or disclose information, the option of doing so electronically when practicable as a substitute for paper and to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content.
E-Government Act of 2002, 44 U.S.C. § 101	Enhances the management and promotion of electronic government services and processes by establishing a broad framework of measures requiring technology to enhance citizen access to government information services.
Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541	Requires Federal agencies to establish agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations.

Executive Orders. The following Executive Orders provide details related to information security for Federal Agencies.

Authority	Description
Executive Order 10450, Security Requirements for Government Employees, April 1953	Establishes that the interests of national security require all government employees be trustworthy, of good character, and loyal to the United States.
Executive Order 13011, Federal Information Technology, July 1996	Establishes policy for the head of each agency to effectively use information technology to improve mission performance and service to the public.
Executive Order 13103, Computer Software Piracy, September 1998	Establishes policy that each executive agency shall work diligently to prevent and combat software piracy in order to give effect to copyrights associated with computer software.
Presidential Decision Directive 63: Critical Infrastructure Protection, May 1998	Requires that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on critical infrastructures, including our cyber systems.

3/21/12 #3941

Replaces 4/15/02 #3397

Authority	Description
Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001	Establishes policy that ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such information systems.

Executive Branch Policy. The policies listed below are established through directives published by the Office of Management and Budget (OMB) based on the applicable laws passed by Congress.

OMB Circular	Description
A-11, Section 53, Information Technology and E-Government	Specifies the identification of security and privacy safeguards for managing sensitive information.
A-123, Management Accountability and Control, as revised December 21, 2004	Specifies the policies and standards for establishing, assessing, correcting, and reporting on management controls in Federal agencies.
A-127, Financial Management Systems, as revised by Transmittal Memorandum Number 3, December 1, 2004	Prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.
A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals	Prescribes policy to agencies for the implementation of the Privacy Act and reporting requirements related to the management of personally identifiable information (PII).
A-130, Appendix III, Security of Federal Automated Information Resources, as revised by Transmittal Memorandum Number 4, November 28, 2000	Stipulates that each agency shall implement a comprehensive automated information security program. The appendix establishes basic managerial and procedural controls that shall be included in Federal automated information systems.

Appendix B  
**NIST Defined Security Control Standards**

<b>IDENTIFIER</b>	<b>SECURITY CONTROL STANDARD</b>	<b>CLASS</b>
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management