

CHAPTER 8 - INFORMATION SECURITY

1. PURPOSE. This document establishes a comprehensive, Agency-wide security program to safeguard Agency information resources. This document sets forth the Agency's information security policy for both manual and automated systems and assigns individual and organizational responsibilities for implementing and administering the program.
2. SCOPE AND APPLICABILITY. This document applies to all EPA organizations and their employees. It also applies to the facilities and personnel of agents (including contractors) of the EPA who are involved in designing, developing, operating, maintaining, or accessing Agency information and information systems.
3. BACKGROUND.
 - a. Information is an Agency asset, just as property, funds, and personnel are Agency assets. The EPA is highly dependent upon its information resources to carry out program and administrative functions in a timely, efficient, and accountable manner.
 - b. The EPA relies on its information collection authority under various enabling statutes to effectively fulfill its environmental missions. The willingness of the regulated community and State and local agencies to supply requested information in a cooperative and timely fashion depends on their confidence that the information will be adequately protected.
 - c. The Agency's information resources are exposed to potential loss and misuse from a variety of accidental and deliberate causes. This potential loss and misuse can take the form of destruction, disclosure, alteration, delay or undesired manipulation. EPA must assure its stakeholders that the integrity and, where necessary, confidentiality of the data they provide will not be compromised. Moreover, the Agency can be subject to acute embarrassment and litigation if certain business or personal information is inadvertently or maliciously disclosed.
 - d. As a result, it is essential that an overall program be established to preserve and adequately protect the Agency's information resources. At the same time, it is equally essential that the program not unnecessarily restrict

information sharing with other Federal agencies, universities, the public, and State and local environmental authorities. Such information sharing has historically played a vital role in the overall fulfillment of the Agency's environmental mission.

- e. The management, control, and responsibility for information resources within EPA are decentralized. Consequently, the management and responsibility for information security are also decentralized. An important example of this is the expanding use of personal computers, networks, distributed data bases and telecommunications. These trends place new responsibilities on office managers, research personnel and others not previously considered information processing professionals. The "computer center" cannot be relied upon to protect Agency operations. Controls must be implemented and maintained where they are most effective.
 - f. In determining responsibilities for information security, it is useful to define a framework of owner/steward/user. Owners are those who create and/or maintain information. Stewards are typically suppliers of information services who possess, store, process, and transmit the information. These roles are often not discrete: the owner is often the principal steward and user of the information.
 - g. All Federal information and information systems are *sensitive* for at least one of three reasons: the need for *availability*, the need for *integrity*, and, where applicable, the need for protection from disclosure (*confidentiality*). Compromising any of these three security goals (i.e., availability, integrity, or confidentiality) may have a significant impact on Agency programs or operations.
4. AUTHORITIES.
- a. Computer Security Act of 1987
 - b. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources
 - c. Privacy Act of 1974, as amended
 - d. Paperwork Reduction of 1995 (P.L. 104-13)

- e. Trade Secrets Act, 18 U.S.C Section 1905
 - f. The Freedom of Information Act of 1974 (5 U.S.C. Section 552)
5. POLICY. It is EPA policy to adequately protect information and information systems, maintained in any medium (e.g., paper, computerized databases, etc.), from improper use, alteration, or disclosure, whether accidental or deliberate. In order to ensure the cost-effectiveness of the security program, information and applications will be protected to the extent required by applicable law and regulation in accordance with the degree of their sensitivity. All EPA information is considered sensitive (See BACKGROUND, section g).
- a. Sensitivity levels for information and information systems (i.e., low, medium, high) shall be determined by the responsible information managers within each organization, as described in Section 4 of the EPA Information Security Manual.
 - b. Information security measures will be applied judiciously to ensure that automated systems security controls operate effectively and accurately and to ensure the continuity of operation of automated information systems and facilities that support critical Agency functions.
 - c. As required by OMB Circular A-130, all major applications and general support systems must have security plans to ensure that appropriate, cost-effective safeguards, commensurate with the level of sensitivity, are in place. Security plans for major applications and general support systems must be updated at least every three years or when a significant change occurs. Security plans shall adhere to the format presented in the EPA Security Planning Guidance document.
 - d. An organization may choose to include multiple general support systems in a single security plan if the general support systems are under the same direct management control and share common functionality.
 - e. Appropriate administrative, physical, and technical safeguards shall be incorporated into all new automated data processing (ADP) application systems (including personal computer-based applications) and major modifications to existing systems.

- f. Appropriate ADP security requirements will be incorporated into specifications for the acquisition of ADP-related services and products.
 - g. Information security awareness and training will be provided within organizational information security programs so that all Agency and contractor personnel are aware of their information security responsibilities.
 - h. Microcomputers which store or process moderately or highly sensitive information must incorporate the safeguards necessary to ensure the protection of the information. If adequate information security cannot be maintained, an alternative system configuration must be used.
 - I. Information security violations will be promptly reported to appropriate officials, and the Inspector General when warranted.
 - j. Contractor personnel who are authorized to bypass significant technical and operational security controls of a system, such as contractor LAN Administrators, shall undergo an appropriate level of background screening by the Office of Personnel Management. Screening shall also be conducted for contractor personnel with authorized involvement in major applications or with authorized access to confidential information.
6. RESPONSIBILITIES.
- a. The Office of Environmental Information is responsible for:
 - (1) Developing and defining the Agency's Information Security Program in accordance with all applicable Federal laws, regulations, and executive orders.
 - (2) Ensuring that all Agency organizations are aware of their compliance responsibilities as they relate to the Agency's Information Security Program.
 - (3) Developing information security awareness training criteria.
 - (4) Providing guidance on selecting and implementing safeguards.
 - (5) Establishing the minimum information security control environment required by the Agency to protect both its ADP resources and its

information from theft, damage, and unauthorized use.

- (6) Establishing and implementing the minimum security controls for EPA's network connectivity (including Internet connectivity) required by the Agency.
- b. Each "Primary Organization Head" (defined by EPA Order 1000.24 as the Deputy Administrator, Assistant Administrators, Regional Administrators, the Inspector General and the General Counsel) is responsible for:
- (1) Establishing an organization-wide information security program to include laboratories and other facilities, consistent with organizational mission and Agency policy. Each Primary Organization Head must ensure that their organization's information security program provides security awareness training based on the security awareness training criteria established by OEI.
 - (2) Ensuring that information and applications within the organization are adequately protected.
 - (3) Ensuring that all general support systems and major applications within the organization (including labs, satellite offices, etc.) have security plans in place and that security plans are updated at least every three years or when a significant change occurs.
 - (4) Providing an annual certification to the Chief Information Officer that security plans are in place and current for each major application and general support system. Certification letters are to be submitted each year during the first week of March.
 - (5) Ensuring the continuity of operations of automated information systems and facilities that support critical functions.
 - (6) Ensuring that appropriate safeguards are incorporated into all new organizational information systems and major modifications to existing systems.
 - (7) Designating Information Security Officer(s) who are knowledgeable in information technology and security.
 - (8) Ensuring that Federal employees and contractor personnel

understand their security responsibilities and that organizational information security regulations are properly distributed.

- (9) Ensuring that all organizational procurements of ADP equipment, software, and services incorporate adequate security provisions.
- c. The Director, Facilities Management and Services Division (FMSD), is responsible for:
- (1) Establishing and implementing physical security standards, guidelines, controls, and procedures in accordance with EPA information security policy.
 - (2) Establishing and implementing standards and procedures for National Security Information in accordance with EPA information security policy and all applicable Federal laws, regulations, and executive orders, including the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.
- d. Office of Grants and Debarment is responsible for:
- (1) Ensuring that Agency interagency agreement policies, solicitations, and award documents contain provisions (as promulgated by OEI) concerning the information security responsibilities of interagency contractors. This also applies to grantees who access EPA information or information systems.
 - (2) Establishing procedures to ensure that interagency contractors (and grantees accessing EPA information or information systems) are in compliance with their information security responsibilities. Violations shall be reported as appropriate to the Project Officer, OEI official, and/or Inspector General. Specific violations involving National Security Information shall be reported to the Director, FMSD, the Inspector General, and the Contracting Officer.
- e. The Office of Acquisition Management is responsible for:
- (1) Ensuring that Agency contract policies, solicitations, and award documents contain provisions (as promulgated by OEI) concerning the information security responsibilities of contractors which may

include submitting to background investigations by the Office of Personnel Management.

- (2) Establishing procedures to monitor contractor compliance with information security responsibilities as specified in contracts let by the Agency.
- f. Each Project Officer (PO), Delivery Order Project Officer (DOPO), and Work Assignment Manager (WAM) is responsible for:
- 1) Ensuring that contractor personnel are aware of their information security responsibilities.
 - 2) Ensuring contractor compliance with information security requirements on individual contracts, delivery orders, or work assignments, respectively. Violations shall be reported as appropriate to the Contracting Officer, OEI official, and/or Inspector General. Specific violations involving National Security Information shall be reported to the Director, FMSD, the Inspector General, and the Contracting Officer.
 - 3) Ensuring that contractors have the appropriate level of background screening when accessing EPA information or information systems under a contract (PO responsibility), delivery order (DOPO responsibility), or work assignments (WAM responsibility).
- g. The Office of Inspector General is responsible for:
- (1) Establishing and implementing personnel security procedures for the screening of all individuals (both Federal and contractor personnel) participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data.
 - (2) Reviewing allegations of waste, abuse, mismanagement, or criminal activity involving information security.
- h. Senior Information Resource Management Officials (SIRMOs) are responsible for:
- (1) Ascertaining that a comprehensive information security program is

implemented for their respective organizations.

- (2) Approving/disapproving information security plans within their organizations.
- I. Information Security Officers (ISOs) are responsible for:
 - (1) Providing SIRMOS with adequate information to determine the effectiveness and appropriateness of information security practices under their purview.
 - (2) Ascertaining that, from an information security perspective, their organization's information is properly managed.
 - (3) Providing organization-wide guidance for security plan development and maintaining the organization's security plan repository.
 - j. EPA Information Managers are responsible for designating sensitivity levels for information, conducting the appropriate security planning and testing activities (including risk assessments and risk analyses where warranted), and ensuring that only authorized individuals access Agency information and information systems.
 - k. Each EPA Manager and Supervisor is responsible for:
 - (1) Ensuring his/her employees are knowledgeable of their information security responsibilities.
 - (2) Ensuring that his/her employees adhere to the organizational information security program established by the applicable Primary Organization Head.
 - l. Each EPA Employee, Contractor, and Grantee is responsible for:
 - (1) Complying fully with his/her information security responsibilities.
 - (2) Limiting his/her access only to information and systems he/she is authorized to see and use.
 - (3) Adhering to all Agency and organizational information security policies, standards, and procedures.

- (4) Reporting information security violations to the responsible Information Security Officer and the Information Manager. Violations involving National Security Information shall also be reported to the Director, FMSD, the Inspector General, and the Contracting Officer.

7. DEFINITIONS.

- a. "Applications Security" means the set of controls that makes an information system perform accurately, reliably, and only those functions it was designed to perform. The set of controls typically includes the following: programming, access, source document, input data, processing storage, output, and audit trail.
- b. "Confidential Business Information" (CBI) includes trade secrets, proprietary, commercial, financial, and other information that is afforded protection from disclosure under certain circumstances as described in statutes administered by the Agency. Business information is entitled to confidential treatment if: (1) business asserts a confidentiality claim; (2) business shows it has taken its own measures to protect the information; (3) the information is not publicly available; or (4) disclosure is not required by statute and the disclosure would either cause competitive harm or impair the Agency's ability to obtain necessary information in the future. Examples include TSCA and FIFRA information and information from the Contracts Payment System.
- c. "Confidential Agency Information" (CAI) includes information used within the Agency that, if not afforded protection from disclosure, could result in unfair contracting practices, or in some way may adversely affect Agency personnel or property. Examples include internal budget information that reveals funds available for various contracting services. Disclosure of this information prior to negotiations could result in inflated contract estimates. Information about an upcoming procurement is confidential and of great value to potential bidders. Also included is information regarding projections or recommendations for personnel changes, whether Federal or contractor, that may cause an individual to become disgruntled and act adversely.
- d. "Confidential Information" is information that requires protection from unauthorized disclosure under Federal statutes. The specific types of

confidential information in EPA are:

- Confidential Business Information (CBI),
 - Confidential Agency Information (CAI),
 - Privacy Act Information,
 - Some Freedom of Information Act-exempt information,
 - Enforcement confidential information, and
 - Budgetary information prior to OMB release.
- e. “General Support System” is an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating systems and utilities, a tactical radio network, or a shared information processing service organization.
- f. "Information" is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including automated, textual, numerical, graphic, cartographic, narrative, or audiovisual forms.
- g. "Information Security" means the protection of information and information resources to ensure their availability, integrity, and confidentiality.
- h. "Information System" means the organized collection, processing, transmission and dissemination of information in accordance with defined procedures, whether automated or manual. This term is used when addressing security requirements that apply to all automated and manual systems.
- I. “Major Application” - is 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. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

- j. "National Security Information" (NSI) means information that is classified as Top Secret, Secret, or Confidential under Executive Order 12958 or predecessor orders, and includes "Restricted Data" and "Formerly Restricted Data" protected under the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act. The specific techniques and responsibilities for NSI are beyond the scope of this policy.
- k. "Personnel Security" involves the use of various techniques, including investigations, to screen both Federal and contractor personnel participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. The level of screening required under OMB Circular A-130 varies from minimal checks to full background investigations depending on the sensitivity of the information to be handled, and the risk and magnitude of loss or harm that could be caused by an individual.
- l. "Physical Security" means the procedures and controls to provide for the protection of personnel, facilities, materials, equipment, and documents against any threat other than overt military action.
- m. "Privacy" is the right of an individual to control the collection, storage, and dissemination of information about himself/herself to avoid the potential for substantial harm, embarrassment, inconvenience, or unfairness.
- n. "Risk Analysis" is a formal methodology to obtain a quantitative measurement of risk to a collection of sensitive data and the people, systems, and installations involved in storing and processing that data. Its purpose is to determine how protective techniques can be effectively applied to minimize potential loss.
- f. "Risk Assessment" is a qualitative determination of risk to a collection of sensitive data and the people, systems, and installations involved in storing and processing that data. Its purpose is to determine how protective techniques can be effectively applied to minimize potential loss.
- p. "Security Violation" means any waste, fraud, abuse, or mismanagement of information resources.
- q. "Sensitive Information" All EPA information is sensitive for at least one of three reasons: the need for *availability*, the need for *integrity*, and, where applicable, *confidentiality*--the need for protection from disclosure. (This

last category includes confidential information; see definition.) The level of sensitivity for EPA's information is rated as low, medium, or high as determined by the responsible information manager.

While EPA does maintain National Security Information (see definition), the specific techniques and responsibilities for NSI are beyond the scope of this chapter.

8. PROCEDURES AND GUIDELINES. Standards, procedures, and guidelines for the Agency's Information Security Program are identified and issued under separate cover in the Information Security Manual. This manual identifies and references, as appropriate, existing procedures in the information security area, such as the Freedom of Information Act Manual, Privacy Act Manual, the Records Management Manual, Confidential Business Information manuals (e.g., the TSCA Security Manual) and Agency Public Information and Confidentiality Regulations at 40 CFR part 2.
9. PENALTIES FOR UNAUTHORIZED DISCLOSURE OF INFORMATION.
 - a. EPA employees are subject to appropriate penalties if they knowingly, willfully, or negligently disclose confidential information (including CBI, CAI, and National Security Information) to unauthorized persons. EPA has legal and regulatory requirements to protect confidential information such as the requirements for protecting CBI at 40 CFR § 2.221. Penalties may include, but are not limited to, a letter of warning, a letter of reprimand, suspension without pay, dismissal, loss or denial of access to confidential information (including National Security Information), or other penalties in accordance with applicable law and Agency rules and regulations, which can include criminal or civil penalties. Each case will be handled on an individual basis with a full review of all the pertinent facts. The severity of the security violation or the pattern of violation will determine the action taken.
 - b. Non-EPA personnel who knowingly, willfully, or negligently disclose confidential information to unauthorized persons may be subject to appropriate laws and sanctions.