

United States
Environmental Protection
Agency

Office of Environmental
Information
Washington, DC 20460

 **EPA EPA Information Security
Manual**

2195A1

1999 Edition

FOREWORD

The Agency recognizes there may be certain parts of the policy which cannot be implemented immediately, as we do not possess the technology to do so. In some instances, the technology may not be sufficiently mature to meet requirements or to be implemented cost effectively. In the interim, compensating management controls must be defined and documented in the security plan or another document cross-referenced in the security plan, **and implemented** to ensure that information is adequately protected.

Many of the requirements in this document have been effective since 1995. However, controls required in this policy should be implemented no later than September 30, 2000, unless a plan for implementation with acceptable time frames has been approved by the Chief Information Officer (CIO). The CIO will work with Program and Regional managers through the planning processes to establish acceptable implementation time frames. In no case may a technical or management control that is in effect on the issuance date of this policy be removed without implementing a substitute control that provides at least the same degree of protection. In addition, the CIO will work with offices to ensure that information is properly categorized according to the availability, integrity, and confidentiality goals in this policy so that appropriate controls can be employed. Where conflicts exist with previously issued EPA policies, this policy supersedes those documents.

EPA INFORMATION SECURITY MANUAL

Table of Contents

SECURITY CONTACT LIST	ii
EXECUTIVE SUMMARY	iv
1.0 INTRODUCTION	1
2.0 EPA'S INFORMATION SECURITY FRAMEWORK	7
3.0 INFORMATION SECURITY CONCEPTS AND PRINCIPLES	11
4.0 INFORMATION SENSITIVITY AND SECURITY GOALS	19
5.0 THREATS	29
6.0 ROLES AND RESPONSIBILITIES	37
7.0 INTERNET USE	49
8.0 PUBLIC ACCESS	55
9.0 FLEXIPLACE	61
10.0 PERSONNEL SECURITY AND TRAINING	67
11.0 TECHNICAL SECURITY	75
12.0 ORGANIZATIONAL SECURITY PROGRAMS	83
13.0 SECURITY PLANS	91
14.0 MANUAL INFORMATION SECURITY	97
APPENDIX A	105
APPENDIX B	111
APPENDIX C	119
APPENDIX D	125
APPENDIX E	135

EPA INFORMATION SECURITY MANUAL

SECURITY CONTACT LIST

This page briefly lists points of contact for security-related incidents, problems, issues, and questions. For general information on these topics, see the section of the Information Security Manual as noted below:

Topic/Question	Information Security Manual Section	Point of Contact
Background Investigations	Section 10 Personnel Security and Training	EPA National Computer Center (NCC) Security Staff
Computer Viruses	Section 5 Threats	LAN Manager
EPA Information Security Program	Section 2 EPA's Information Security Framework	National Program Manager for Information Security
Flexiplace Requirements	Section 9 Flexiplace	Supervisor
Hacker Incidents and Virus Alerts or Warnings	Section 5 Threats	EPA's Computer Emergency Response Team (CERT) (919) 541-7862
Internet Security	Section 7 Internet Use	National Computing Center (NCC) Security Staff
Organizational Security Programs	Section 12 Organizational Security Programs	Senior Information Resource Management Official (SIRMO)/ Information Security Officer (ISO)
Security Plan Development	Section 13 Security Plans	Information Manager (i.e., System or Application Manager).
Security Plan Approval	Section 13 Security Plans	SIRMO
Security Awareness Training	Section 10 Personnel Security and Training	ISO

Other Security-Related Topics

Points of Contact

Bomb Threats, in any form,
i.e., electronic, telephone, etc.

Facilities Management and Services Division
(202) 260-2013

Misuse of Information Resources

Supervisor

Security Plan Reviews

Section 13, Security Plans

System Problems

System or LAN Manager

Waste, Fraud, and Abuse

Office of Inspector General

EXECUTIVE SUMMARY

The United States (U.S.) Environmental Protection Agency (EPA) depends heavily on information and information technology (IT) to accomplish the Agency's mission. The collection, processing, and maintenance of this information has been entrusted to EPA and is paid for by U.S. taxpayer dollars. Information, in any form, is a valuable Agency asset. As with any valuable asset, care must be taken to ensure that information retains its value and the use for which it was originally obtained.

Supporting EPA's Mission

EPA depends on its information and automated information resources to fulfill its mission. The lack of security in Agency general support systems and major applications can have a significant impact on the Agency's ability to achieve its mission. Much of EPA's environmental information is provided by its stakeholders, including state and local governments and the regulated community. EPA must assure its stakeholders that the integrity and, where necessary, confidentiality of the data they provide will not be compromised. The inability to provide this assurance would undermine EPA's credibility.

Support for Agency Initiatives

EPA's information resources provide vital support to achieving Agency initiatives such as electronic reporting and public access. Electronic reporting depends on the ability to secure data as it enters EPA's data processing environment, authenticate the supplier of the data, ensure non-repudiation, and maintain a chain of custody to ensure that data can be used for enforcement actions if necessary. For EPA's public access initiatives to be successful, the Agency's information systems must provide accurate and timely information while ensuring that EPA information resources are protected from unauthorized access and modification.

Framework for EPA's Information Security Program

The Agency's security framework is composed of EPA's policies, standards, procedures, and guidance for information security. These are set forth in multiple Agency documents, including the following: Chapter 8 of the EPA *IRM Policy Manual (Directive 2100)*, *EPA Information Security Manual (ISM) (Directive 2195)*, *EPA Information Security (InfoSec) Program Plan*, *EPA Information Security Awareness Training Addendum*, *EPA Information Security Planning Guidance*, and *EPA Standards of Behavior for the Security of Information Resources*.

National and Organizational Information Security Programs

EPA has two primary layers of Information security programs: the **National Information Security (InfoSec) Program** and **organizational information security programs**. The Agency's National InfoSec Program is administered by the Office of Environmental Information (OEI). The National InfoSec Program develops and defines an Agency-wide information security program in accordance with applicable Federal laws, regulations, and executive orders. In addition, the National InfoSec Program defines the minimum information security

EPA Information Security Programs,
Continued

control environment required by the Agency to protect both its Automated Data Processing (ADP) resources and its information from theft, damage, and unauthorized use.

Organizational information security programs must be established by Primary Organization Heads. These organizational programs must be consistent with the organization's mission and based on the information processed, the manner in which the information is used, computing platforms, and associated risks and vulnerabilities in the respective organization.

Roles and Responsibilities

Individuals throughout EPA have information security responsibilities. As previously stated, the Primary Organization Head is responsible for establishing an organizational information security program. Senior Information Resources Management Officials (SIRMOs) are responsible for implementing and administering their organization's information security program. Information managers are responsible for preparing information security plans. Information Security Officers (ISOs) are responsible for ensuring that information security programs in their organizations are current. Individuals using EPA systems are responsible for the security of the information they use. The ISM provides the baseline information to carry out these responsibilities.

Security Plans

Information systems face a wide range of threats that can compromise information availability, integrity, and confidentiality. Acts of nature such as lightning, tornados, and floods may damage hardware or halt application processing. Unethical individuals can destroy data and hardware, plant viruses or malicious code, and disclose confidential information. Accidents and errors can compromise Agency information. Security plans provide the means for management to evaluate risks and ensure that systems are adequately protected.

Document Scope

This ISM contains the required policies, standards, procedures, and guidelines to ensure comprehensive Agency information security programs. A comprehensive program will assist EPA in achieving its environmental mission, goals, and administrative support needs. Ensuring the availability of information assists EPA in its goal to provide responsible public access to environmental data. Protecting the integrity of the Agency's information ensures continued leadership in the nation's science, research, and assessment efforts; helps the Agency and Congress make sound regulatory and program decisions; and assists in carrying out EPA's programs and policies. Ensuring the confidentiality of the Agency's data, where required, supports enforcement activities and reinforces the confidence that EPA's State partners and data submitters place in its ability to protect their data.

Document Scope,

This ISM applies to all EPA organizations and their employees. It also

EXECUTIVE SUMMARY

continued

applies to the facilities and personnel of EPA agents (including contractors) who access EPA information and information systems, or who are involved in designing, developing, operating, or maintaining Agency information systems.

1.0 INTRODUCTION

The Environmental Protection Agency (EPA) relies on information in both manual and automated form to achieve its mission. The Agency collects and processes vast amounts of information to implement its programs and measure their success, as well as manage and support its daily activities. EPA's information must be accurate, reliable, and accessible to authorized users for the Agency to meet its mission and goals.

This Section provides an overview of the Information Security Manual and its purpose, scope and applicability, and organization.

1.1 BACKGROUND

EPA uses automated and manual information systems to collect, process, store, and disseminate environmental, programmatic, financial and other administrative information. EPA defines an information system as the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

EPA's policy is to protect information maintained in *any* medium (e.g., paper, computerized data bases, etc.) from improper use, alteration, or disclosure, whether accidental or deliberate.

When addressing security requirements in this EPA Information Security Manual (ISM), the term "information system" refers to all automated and manual systems. Specific requirements in this manual, such as security plans, are directed at automated systems in particular. This set of automated systems includes general support systems and major applications (defined in Appendix D).

1.2 PURPOSE

The ISM defines EPA's information security policy based on Chapter 8 of the EPA *Information Resources Management (IRM) Policy Manual*, Directive 2100. The two primary objectives of the ISM are to:

- C Set forth the requirements and provide guidance for securing Agency information resources in accordance with EPA and Federal security policies and mandates.
 - C Define the security responsibilities of all personnel who use Agency information or use, develop, operate, or maintain EPA information systems.
-

**1.3
SCOPE AND
APPLICABILITY**

All EPA personnel are responsible for protecting the Agency’s information resources. Security for the Agency’s information must be applied at all levels—from the Agency’s Information Security Program to organizational programs and individuals.

This ISM applies to all EPA organizations and their employees. It also applies to the facilities and personnel of EPA agents (including contractors) who access EPA information and information systems, or who are involved in designing, developing, operating, or maintaining Agency information systems.

**1.4
EPA
INFORMATION
SECURITY
MANAGEMENT
STRUCTURE**

EPA's management structure includes the following four tiers for administering information security:

- C Senior EPA Managers
- C Senior Information Resources Management Official (SIRMO)
- C Information Security Officer (ISO)
- C Information Manager

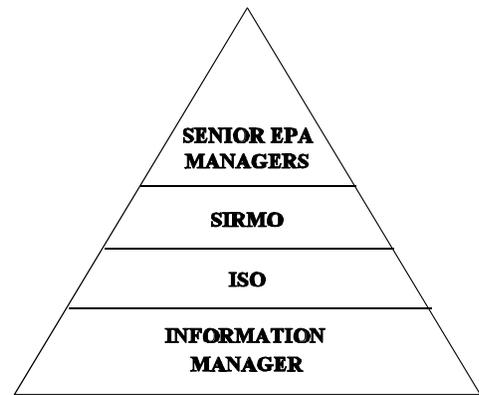


Figure 1-1. EPA Information Security Management Structure

Figure 1-1 illustrates the Information Security Program Management Structure. The following sections briefly discuss these roles. See Section 6 for specific roles and responsibilities.

**SENIOR EPA
MANAGERS**

Senior EPA managers, including Assistant Administrators, Regional Administrators, Division Directors, and Office Directors make up the top-most level of EPA's information security management structure. EPA’s senior management is responsible for establishing organizational security programs to ensure that the information resources within their purview are adequately protected.

SIRMO

The second level of EPA's information security management structure is the SIRMO. The SIRMO implements and administers their organization’s

SIRMO, Continued

information security program. The SIRMO also directs and manages information resources planning and budgeting, and ensures that information system acquisitions within their organization complies with Federal and EPA-specific policies and regulations.

ISO

The next security management tier is that of the ISO. The ISO is designated by the Assistant Administrators (AA), Regional Administrators (RA), the Inspector General (IG), or the General Counsel for their respective organizations. The ISO ensures that information resources under his/her purview are managed and protected appropriately.

INFORMATION MANAGER

The final security management tier is the Information Manager. The Information Manager is assigned by the EPA office responsible for management and oversight of the program area or administrative activity.

T Information Owners/Sponsors

As noted on the left, Information Managers can be classified as information owners, information stewards, or EPA support system or application managers/stewards/sponsors.

T Information Stewards

When information clearly belongs to EPA, the Information Manager is an information owner or sponsor. Sponsor or owner responsibilities are likely to include the initial input, maintenance, release, archiving, and final destruction of the information. An Information Manager is in a stewardship role when the information belongs to a party other than the Agency, such as information owned by and provided to the Agency by States. A steward is responsible for managing and using the information. Information Managers also include Agency personnel who manage or sponsor Agency support systems and applications that provide data processing services to other Information Managers.

T EPA Support System and Application Managers/Stewards/Sponsors

In all cases, the information manager is responsible for ensuring that the information is managed and protected in a manner that is consistent with EPA's policies and standards.

ORGANIZATIONAL SECURITY PROGRAMS

While the Office of Environmental Information (OEI) administers EPA's National Information Security Program, each EPA organization is responsible for organization-specific information security policies and procedures. EPA organizations with statutory authority for certain types of information may issue security procedures dealing

SECTION 1.0 INTRODUCTION

ORGANIZATIONAL SECURITY PROGRAMS, *Continued*

exclusively with that information. For example, the Office of Prevention, Pesticides, and Toxic Substances is responsible for Toxic Substances Control Act (TSCA) confidential business information.

Section 12 of the ISM presents the procedures for EPA Program and Regional Offices to use in establishing organizational information security programs. Specialized information security procedures developed by EPA organizations may expand on the ISM's core information security requirements, but all organizational security procedures must still satisfy the requirements specified by the ISM. EPA employees and contractors must adhere to the procedures presented in the ISM and, as appropriate, to the specialized information security procedures established in particular program areas.

1.4 DOCUMENT ORGANIZATION

The ISM provides an introduction to information security and discusses EPA's security framework. Subsequent portions of the ISM explain key security concepts and provide EPA's policy and procedures for ensuring that all EPA information resources are adequately protected. The ISM is organized into the following 14 sections:

Section	Topic
1.0	Introduction
2.0	EPA's Information Security Framework
3.0	Information Security Concepts and Principles
4.0	Information Sensitivity and Security Goals
5.0	Threats
6.0	Roles and Responsibilities
7.0	Internet Use
8.0	Public Access
9.0	Flexiplace
10.0	Personnel Security and Training
11.0	Technical Security
12.0	Organizational Security Programs

DOCUMENT	Section	Topic
ORGANIZATION, <i>Continued</i>	13.0	Security Plans
	14.0	Manual Information Security

The ISM includes the following five appendices:

Appendix A - Continuity of Support and Contingency Planning

Appendix B - Annotated References

Appendix C - Information Security Resources

Appendix D - Acronyms and Definitions

Appendix E - Index

[This page intentionally blank.]

2.0 EPA'S INFORMATION SECURITY FRAMEWORK

The Agency's information security framework is composed of EPA's policies, standards, procedures, and guidance for information security. These are set forth in multiple Agency documents, including the following:

- C Chapter 8 of the EPA *IRM Policy Manual*
- C EPA *Information Security Manual*
- C EPA *Information Security (InfoSec) Program Plan*
- C EPA *Information Security Awareness Training Addendum*
- C EPA *Information Security Planning Guidance*
- C EPA *Standards of Behavior for the Security of Information Resources*
- C EPA *Risk Analysis Guidance*

This Section summarizes EPA's information security framework. This framework is founded on the policies, procedures, and guidance set forth in Agency documents. These documents define security requirements and practices from policy level through implementation.

In addition, many EPA organizations have programmatic documents containing standards, procedures, and guidelines for information security. Examples of these types of program-specific documentation include the *Toxic Substances Control Act (TSCA) Confidential Business Information Security Manual*, *Records Management Manual*, *Privacy Act Manual*, and *Freedom of Information Act Manual*. EPA procedures and guidance that impact the Agency's Information Security Program include the *National Technology Services Division (NTSD) Operational Directives Manual*.

While all Information Security Program documents address information security issues within the Agency, each approaches issues from different levels. Some documents are purely strategic, while others provide specific policies, procedures, and/or guidance. For example, while the *IRM Policy Manual* mandates security plans, this Security Manual presents specific security planning requirements. EPA's security planning guidance document (*Information Security Planning Guidance*) takes the process to another level—it describes the process, explains what the process will achieve, and provides detailed guidance for completing security plans for general support systems and major applications. Together, these documents carry the process through from policy to implementation.

The following subsections provide brief descriptions of the documents that are the foundation of EPA's InfoSec Program.

2.1 EPA IRM POLICY MANUAL (EPA DIRECTIVE 2100)

The EPA *IRM Policy Manual*, Chapter 8, establishes the Agency's Information Security Program and defines the Agency's Information Security Policy. EPA policy is to ensure that all Agency information maintained in any medium (e.g., paper, computerized databases, etc.) is protected commensurate with the risk and magnitude of the harm resulting

**EPA IRM POLICY
MANUAL,
Continued**

from the loss, misuse, or unauthorized access to or modification of EPA's information. Chapter 8 further defines the activities required to protect EPA's information, support systems, and applications; establishes responsibilities; and identifies components of the InfoSec Program.

Other chapters within the *IRM Policy Manual* address objectives, responsibilities, and procedures for information security in other aspects of EPA's IRM program, including records management, privacy of individuals, and system life cycle management.

**2.2
EPA
INFORMATION
SECURITY
MANUAL (ISM)**

The ISM addresses the operational aspects of the policy listed in Chapter 8 of the *EPA IRM Policy Manual*. The ISM explains important components of the policy and provides detailed policy, procedures, and guidance for meeting Federal security mandates and the Agency's Information Security Policy.

The ISM defines the processes EPA relies on to protect its information resources and identifies the information security responsibilities for key personnel throughout the Agency. The ISM deals with all information assets—whether paper, electronic, or other form.

**2.3
INFORMATION
SECURITY
PROGRAM PLAN**

The Information Security Program Plan provides the strategic direction for implementing information security at EPA. The plan describes the InfoSec Program strategy, defines the Program's current status, and outlines the objectives of the Program.

**2.4
INFORMATION
SECURITY
AWARENESS
TRAINING
ADDENDUM**

EPA's *Information Security Awareness Training Addendum* defines the framework and overall requirements for EPA's Information Security Awareness Program. Security awareness and training requirements are set forth in the following laws and regulations:

- C Computer Security Act of 1987 (P. L. 100-235).
 - C The Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
 - C Code of Federal Regulations (CFR), Title 5, Chapter 1, Part 930, Subpart C, *Employees Responsible for the Management or Use of Federal Computer Systems*.
-

**INFORMATION
SECURITY
AWARENESS
TRAINING
ADDENDUM,
*Continued***

EPA's Information Security Awareness document is an addendum to EPA's InfoSec Program Plan and provides instructions for use by EPA organizations in fulfilling security awareness training requirements.

The National Institute of Standards and Technology (NIST) provides security training guidance based on the above laws and regulations. The NIST training guidance is available on the NIST Computer Security Research Clearinghouse web site. The URL is: <http://csrc.nist.gov/>

**2.5
STANDARDS OF
BEHAVIOR**

EPA's *Standards of Behavior for the Security Of Information Resources* provides EPA personnel with a set of principles, or code of conduct, to follow during day-to-day operations. The Standards document also provides guidance on developing rules of behavior for Agency general support systems and major applications. Appendix III of the Office of Management and Budget (OMB) Circular A-130 defines the requirements for rules of behavior and how rules are to be incorporated into general support systems and major applications' security plans. The Standards document provides models that can be used, or tailored for use, in developing rules of behavior that meet Appendix III requirements.

**2.6
GUIDELINES**

Guidelines used within the Information Security Program are methods of implementing the ISM. Guidelines describe how specific activities within the Program may be conducted. Guidelines are not, in and of themselves, policy documents—rather, they explain how policy may be followed. Guidelines are intended to provide detailed assistance to EPA personnel in effectively fulfilling their information security responsibilities. Guidelines include, but are not limited to, EPA's *Information Security Planning Guidance* and *Risk Analysis Guideline*.

**2.6.1
INFORMATION
SECURITY
PLANNING
GUIDANCE**

Security plans are required for all general support systems and major applications. EPA's *Information Security Planning Guidance* describes Federal and Agency security planning requirements and the four required controls for the security of information systems: assignment of responsibility, security plans, authorization to process, and periodic security control reviews. The Planning Guidance provides instructions for developing security plans for general support systems and major applications. Security plan developers **must adhere to the security plan format** as set forth in EPA's *Information Security Planning Guidance*.

2.6.2
RISK ANALYSIS
GUIDELINE

In cases where a full formal risk analysis is warranted, the EPA *Risk Analysis Guideline* provides an approach for conducting risk analyses of EPA's automated information systems. Generally, formal risk analysis should be completed for information systems where risks or the magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of information would be significant.

The *Risk Analysis Guideline* provides worksheets for identifying an information system's security characteristics and baseline security requirements. The *Risk Analysis Guideline* also includes worksheets for identifying threats, vulnerabilities, and the additional controls needed to reduce the level of risk. The EPA *Risk Analysis Guideline* is a companion document to the ISM.

3.0 INFORMATION SECURITY CONCEPTS AND PRINCIPLES

Ensuring the security of information resources requires a thorough understanding of security concepts and use of basic security principles. These principles are particularly important to protecting EPA information resources from loss, misuse, unauthorized access or modification commensurate with their importance to the Agency.

Section 3.0 defines two key information security concepts: information sensitivity and security goals. This Section also outlines basic security principles for individuals to follow to ensure that EPA information resources are adequately protected.

The information system development process must consider information security throughout the life-cycle. The security concepts, principles, and requirements presented in the ISM apply to all stages of the information system life cycle, from initiation through retirement. Just as adding requirements late in the design phase increases the time and cost to implement a system, so too does retrofitting information security requirements into an application or system that is already operational. In addition, retrofitted security controls are often much less effective than those identified and implemented at the initiation of an information system. Therefore, EPA and EPA contractor personnel must ensure that information security is assessed and incorporated at all stages of the life cycle.

This section discusses the following two key information security concepts: information sensitivity and security goals. In addition, this section presents security principles for individuals to follow in ensuring that EPA's information is adequately and cost-effectively secured.

3.1 BASIC SECURITY CONCEPTS

T **Information
Sensitivity**

T **Security
Goals**

Information Sensitivity: Consistent with OMB Circular A-130, Appendix III, all Agency information is sensitive. EPA's information is sensitive because the loss, misuse, or unauthorized access to or modification of EPA's information could adversely affect the Agency's ability to conduct its programs or ensure personal privacy as specified in the Privacy Act.

All Federal information and information systems are sensitive for at least one of three reasons: the need for availability, the need for integrity, and/or the need for protection from disclosure (confidentiality).

The phrase "sensitive information" is sometimes thought to include only confidential information that must be kept from unauthorized disclosure. However, in the context of information security, the phrase also refers to information availability and integrity.

L Note:

National Security Information is not addressed in this Manual.
This manual does not address the security requirements for classified information. Special provisions for the protection of classified information—National Security Information (NSI)—are beyond the scope of this manual and are available from the EPA Facilities Management and Services Division (FMSD). FMSD establishes policy on the methods of protection required for NSI.

Security Goals

Sensitive information has the following three security goals: ensuring information **availability**, protecting information **integrity**, and ensuring that the **confidentiality** of information is not compromised.

- C **Availability** refers to the ability of all authorized users to access the information when needed. Protecting information availability means ensuring that access to information and required computing services is not denied. For example, payroll information and associated computing capabilities must be available in a timely manner if paychecks are to be issued on payday.

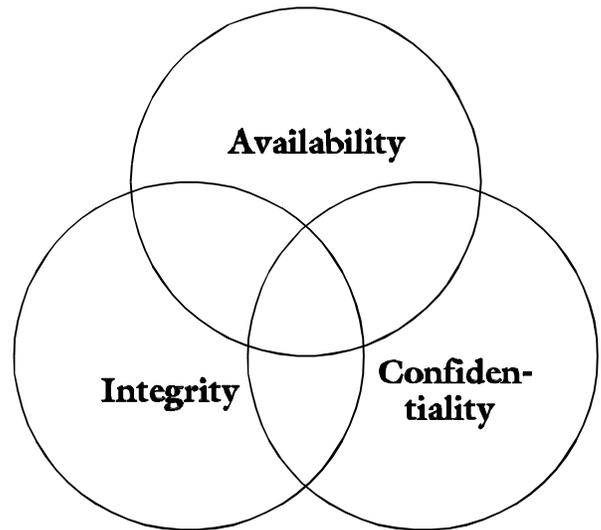


Figure 3-1. Security Goals

- C **Integrity** refers to the original content and composition of data. Ensuring information integrity means protecting data from unauthorized or accidental alteration. Payroll information is one example of information for which integrity is important.
- C **Confidentiality** refers to the need to prevent unauthorized disclosure of certain types of information. Privacy Act information is an example of information that must be kept from unauthorized disclosure.

BASIC SECURITY

The purpose of the EPA InfoSec Program is to establish and maintain these

CONCEPTS,
Continued

goals for information in Agency information systems.

Figure 3-1 illustrates the interrelationships between information security goals.

L Note:

EPA information shall be protected based on a defined level of availability, integrity, and confidentiality.

Information and related information systems may have one or more security goals simultaneously. For example, information that requires controls to ensure its integrity (protection from unauthorized or unintentional modification) may, at the same time, require controls to ensure its confidentiality (protection from unauthorized disclosure). In addition, information security goals may change over the course of the information's life cycle (i.e., creation, collection, etc.). Section 4 discusses these goals in more detail.

3.2
SECURITY
PRINCIPLES

This subsection discusses security principles for effective information security programs. These principles are founded in the basic security concepts previously discussed. The following security principles are presented in this subsection.

- C *Risk management*
- C *Adequate security*
- C *Cost-effective security*
- C *Least privilege*
- C *Accountability*
- C *Authorized use*
- C *Ethical behavior*

Risk
Management

All EPA personnel must use a risk management approach to protect their information. Risk management means identifying risks, identifying an acceptable level of risk, and maintaining risks at that level. *An acceptable level of risk is the point at which the risk is more acceptable than the cost to mitigate the risk (in dollars or its affect on the ability to use the*

Risk

information system). Risk management, adequate security, and cost-

*Management,
Continued*

effective security are closely related. All of these concepts require identifying security controls that are effective in controlling risk for a reasonable cost.

A risk management approach (maintaining risks at an acceptable level) requires risks to be identified and assessed through a **risk assessment** or a **risk analysis**. The difference between a risk analysis and a risk assessment is that a *risk analysis* typically follows a formal methodology to obtain a quantitative measurement of risk; while a *risk assessment* uses a qualitative determination of risk.

Formal risk analyses are no longer required for all Agency information systems. However, risk analyses are required for large, complex information systems or those for which the harm resulting from the loss, misuse, or unauthorized access to or modification of the information system and its information would be significant. In these instances, a risk analyses is required to ensure that risks are adequately identified and controlled.

Both risk analyses and assessments generally include the following activities:

- C Determining the value of information assets, e.g., information, hardware, software, etc. (based on an inventory of assets).
- C Determining the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
- C Identifying threats and vulnerabilities.
- C Assessing the effectiveness of current security controls in protecting against the identified threats and vulnerabilities.
- C Identifying additional security controls required to protect against the identified threats and vulnerabilities.
- C Justifying and documenting an analysis which supports any waiver of materiality requirements.

The level of detail included in a risk assessment must be based on the sensitivity of the information and its value to the organization to ensure that information and information system resources are adequately protected.

*Adequate
Security*

All individuals owning, managing, or accessing EPA's information must ensure that the information is provided adequate security. Appendix III of

OMB Circular A-130 defines adequate security as follows:

“security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.”

Security controls must be implemented to protect information’s availability, integrity, and confidentiality. Information must not be copied or transferred to another computing platform if adequate security cannot be maintained. Information can only be shared if it can be provided security comparable to the level of protection that it had in its original information system.

Cost-Effective Security

Owners, managers, and users of EPA’s information resources must ensure that resources are adequately protected through the use of cost-effective security controls. “Cost effective” in this context means that security controls provide an adequate level of protection for the amount of money and time invested in the control. Security controls—both administrative and technical controls—are determined to be cost-effective based on the following formula:

$$C_c \sim T_l \cdot L_p$$

Where:

C_c = cost of the control

T_l = the likelihood of threat occurrence

L_p = potential loss

L Note:

Potential loss may include monetary value, impact on an organization’s mission, loss of time, adverse impact on public perception, etc.

Given the differences between the types and sensitivity of information processed and computing platforms used throughout EPA, a security control that is cost-effective for one information system may not be cost-effective for another.

Least Privilege

The principle of least privilege is limiting the level of access to information resources (such as information systems, applications, databases, or records and processing capabilities) to the specific level necessary to perform the

assigned functional duties. Applying this principle at EPA means that individuals must be limited to only those information resources that they are authorized to access based on their job responsibilities. An example of this principle is generally followed in configuring LAN access authorities. Individuals are authorized access to a LAN, but are not provided access rights to all directories and file structures. These individuals are only provided access rights to the directories and file structures they need to complete their jobs.

Accountability

Everyone who uses or manages EPA's information must be held accountable for his/her actions while using the Agency's information systems. EPA holds information system users accountable for unauthorized activities. Unauthorized activities may result in intentional or unintentional damage, inappropriate disclosure, or denial of access to information resources, often referred to as denial of service. Information system owners and managers must ensure that there is a positive means of identifying each user. General support systems and major applications must have audit trails that maintain a record of each user's activities while accessing the system or application. Audit trails must be reviewed regularly to ensure that users are held accountable for their actions.

***Authorized
Access***

Many EPA information systems contain confidential data (e.g., enforcement data, confidential business information, and Privacy Act data). In addition, many Agency information systems contain information that must be protected from accidental or intentional modification (e.g., payroll data). To protect these categories of information, Agency information systems must be planned, designed, and operated on the basis that only authorized individuals will be allowed access.

Where the application promotes or permits public access, authorization must be obtained to ensure that only the appropriate types of information are made available to the public. The necessary authorization must be obtained from the Information Manager and the Division Director of the general support system which will be providing access to the public.

***Authorized
Access,
Continued***

Information that is *not* appropriate for release to the public includes information that is required by law or regulation to be protected or other information of a confidential nature.

***Ethical
Behavior***

The availability, integrity, and confidentiality of EPA's information depends in a large part on the behavior of those individuals who access and use the information. All EPA staff must use information resources and access information systems in an ethical manner. Ethical use of the Agency's information resources includes following the standards listed below:

- C Use only the information needed to complete the job. Follow EPA's policies and the system or application rules of behavior (as defined in the security plan - see Section 13) for viewing, accessing and disposing of information according to its security goal and level of sensitivity.
- C Use information systems in a manner that will not deny services to other users. While Internet news groups may provide a wealth of information on environmental topics, the flood of incoming and outgoing mail may affect the system's ability to fill other users' requests for system services.
- C Protect confidential information from unauthorized disclosure.
- C Protect the availability and integrity of EPA's information.
- C Follow the user ID and password policies established for the information system accessed. Remember, users will be held accountable, based on their user ID and password, for their actions while using the information system.
- C Protect software and hardware from damage, abuse, and unauthorized use.
- C Attend security training and stay abreast of security policies and requirements.
- C Report all security incidents and violations to the proper authorities.

[This page intentionally blank.]

4.0 INFORMATION SENSITIVITY AND SECURITY GOALS

The first step in providing adequate and cost-effective security for EPA's information is to determine the degree to which information is sensitive (i.e., how important the information is) and the requirement for information availability, integrity, and, where applicable, confidentiality. Section 3 of this manual discusses security goals at a high level. This section expands on the discussion and provides criteria to be used by owners and users of EPA's information to determine which security goals apply to their information.

This Section discusses the concept of information sensitivity and provides guidance for identifying information security goals—availability, integrity, and confidentiality.

4.1 INFORMATION SENSITIVITY

As discussed in Section 3.0, all EPA information is sensitive because it requires at least some level of protection to ensure its availability, integrity, and, where applicable, confidentiality. The sensitivity of information must be determined to ensure that the information is protected commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.

L Note:

Determining information sensitivity means determining the degree to which the availability, integrity, and, where applicable, confidentiality of the information is important. In the case of information that is available to the public (e.g., public access) confidentiality is not a concern (See Section 4.5).

The sensitivity of information is based on its importance to the organization, its mission, and daily operations. The level of sensitivity must take into account the degree to which availability, integrity, and confidentiality are important for the information.

High, Medium, or Low

The level of sensitivity is stated as high, medium, or low. This is a qualitative assessment of the overall sensitivity of information based on the most important security goal(s) identified. For example, information for which integrity is a critical (high) concern would be referred to as highly sensitive.

4.2 WHY IDENTIFY SECURITY GOALS? WHY IDENTIFY

Identifying applicable information security goals—availability, integrity, and confidentiality—is necessary to ensure adequate, cost-effective security. The determination of which security goals are important and the degree to which they are important is used in selecting effective security measures.

SECURITY GOALS?

Continued

Consider, as an example, environmental information made available to the public. Information availability is an important security goal for this information. If the information must be available within 24 hours, then security measures must be used to ensure the information will be available as needed.

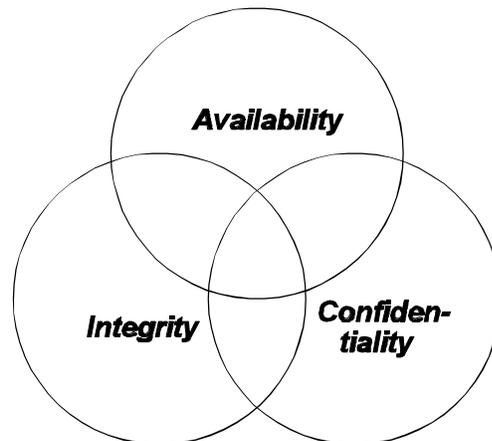
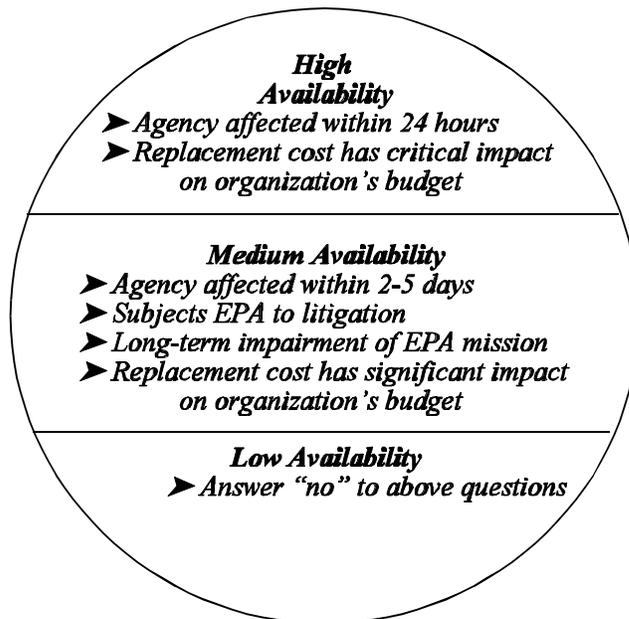


Figure 4-1. Security Goals

Information has one or more security goals as illustrated in Figure 4-1. Payroll information is an example of information for which all three security goals are required. The integrity of the information must be assured, the information must be available in order to complete paychecks, and some of the information is confidential (Privacy Act information). In addition, information of different types and belonging to different organizations may have these goals to different degrees. Consider a public access information system as an example. The requirement for availability is high—the information must be readily available when requested.

The following sections provide the criteria used to determine which security goals apply to an organization's information and whether the sensitivity is high, medium, or low.



4.3 AVAILABILITY

Availability refers to the ability of all authorized users to access information when needed. Providing security controls to ensure information availability is essential for information

SECTION 4.0 INFORMATION SENSITIVITY AND SECURITY GOALS

AVAILABILITY,
continued

that must be accessible on a timely basis to meet mission requirements or avoid substantial loss. The graphic summarizes the criteria used to determine if the information has an availability requirement and the degree (high, medium, or low) to which the security goal is important. An example of information requiring a high level of availability is payroll information. Information availability as a primary security goal.

**IDENTIFYING
AVAILABILITY
REQUIREMENTS**

Answers to the following questions will help determine if the requirement for the availability information security goal is high or medium. An answer of “yes” to any one question within a sensitivity level, will determine the level of sensitivity for this goal. If the answers to these questions are “no,” then the availability requirement is probably low.

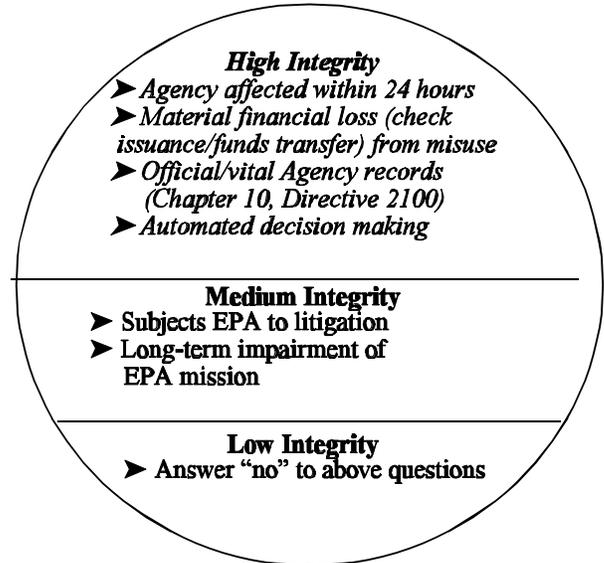
AVAILABILITY	
High	C Could the Agency be affected immediately (within 24 hours) if the information were unavailable?
	C Would the cost of recreating the information, information system, or processing environment, as determined by the information manager, have a critical impact on the organization's budget?
Medium	C If the information were unavailable, could the Agency experience an impact within 2 - 5 days?
	C If the information were unavailable, could the Agency be subject to litigation?
	C If the information were unavailable, could it impair the Agency's long-term ability to accomplish its mission?
	C Would the cost of recreating the information, information system, or processing environment, as determined by the information manager, have a significant (but not critical) impact on the organization's budget?
Low	C Answers to the questions above are “no.”

**4.4
INTEGRITY**

Maintaining information integrity refers to keeping information “unaltered,” i.e., free from unauthorized or accidental modification or destruction. All information has integrity requirements; inappropriately changed or modified data, or system and application software, impacts information integrity and compromises the value of the information system.

The graphic on the right summarizes the criteria used to determine if information has integrity as one of its security goals and the degree (high, medium, or low) to which the security goal is important. Examples of information requiring protection to preserve integrity include the following:

- C Financial information
- C Law enforcement
- C Environmental information



Because of the importance of the Agency's information to the environmental decisions made by the Agency, its partners, and the public, it is EPA's responsibility to ensure that the information is, and remains, as accurate and credible as possible.

Information designated less than high integrity because a loss of monetary assets is not considered material, must be justified by analysis and documentation.

L Note:

**IDENTIFYING
INTEGRITY
REQUIREMENTS**

Answers to the following questions will help determine if the requirement for the information security goal of integrity is high or medium. An answer of “yes” to any one question within a sensitivity level, will determine the level of sensitivity for this goal. If the answers to these questions are “no,” then the integrity requirement is probably low.

**IDENTIFYING
INTEGRITY**



SECTION 4.0 INFORMATION SENSITIVITY AND SECURITY GOALS

REQUIREMENTS,
Continued

High	C	Would EPA be affected immediately (within 24 hours) if the information was inappropriately modified?
	C	Is the information required for issuing checks or transferring funds, such that misuse could result in a material loss of monetary assets?
	C	Based on program criteria, is the information required for automated decision making such as ordering supplies or controlling the Agency's assets?
	C	Based on Chapter 10 of the IRM Policy Manual, is the information: <ul style="list-style-type: none"> - An <i>official record of the Agency</i>? - Information that is vital to the essential functions of the Agency during an national emergency or essential to the legal rights and interests of individual citizens and the Government?
Medium	C	If the information were incorrect or otherwise corrupt, could the Agency be subject to litigation?
	C	If the information were incorrect or otherwise corrupt, could it impair the Agency's long-term ability to accomplish its mission?
Low	C	Answers to the questions above are "no."

4.5
CONFIDENTIALITY

Confidentiality refers to prevention of unauthorized or inappropriate disclosure of information. The graphic on the right summarizes the criteria used to determine if the information has a confidentiality requirement and the degree (high, medium, or none) to which this security goal is important. Certain types of Agency information must be protected from unauthorized or accidental disclosure. EPA's confidential information includes, as a minimum the following:

- C Confidential Business Information (CBI)
- C Confidential Agency information (CAI)

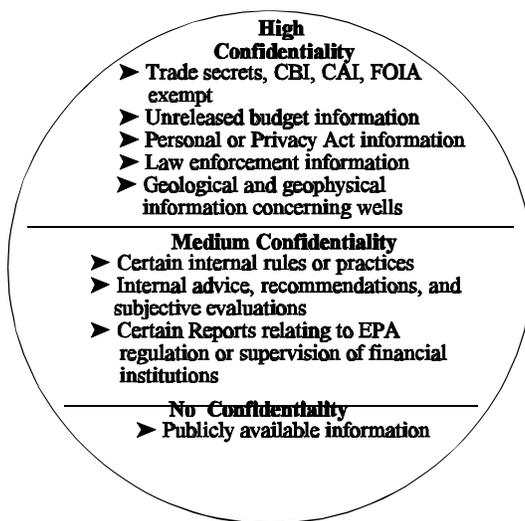
CONFIDENTIALITY,
Continued

- C Privacy Act information
- C Enforcement-confidential information
- C Budgetary information prior to OMB release
- C Certain other information exempt from disclosure under the *Freedom of Information Act* (FOIA), also referred to as FOIA-exempt information. Offices may determine that specific categories of FOIA-exempt information must be treated as confidential (40 C.F.R 2).

Definitions for the above terms, including FOIA-exempt, can be found in Appendix D, Glossary.

IDENTIFYING CONFIDENTIALITY REQUIREMENTS

Answers to the following questions will help determine if the requirement for the information security goal of confidentiality is high or medium. An answer of “yes” to any one question within a sensitivity level, will determine the level of sensitivity for this goal. If the answers to these questions are “no,” then a confidentiality requirement does not exist (i.e., the information is available to the public).



CONFIDENTIALITY	
High	C Is the information Confidential Business Information (CBI)?
	C Does the information pertain to budgets previously unreleased by OMB or other authorities?

IDENTIFYING CONFIDENTIALITY

CONFIDENTIALITY (Continued)	
High,	C Does the information pertain to personnel or medical

SECTION 4.0 INFORMATION SENSITIVITY AND SECURITY GOALS

REQUIREMENTS,
Continued

C	Is the information subject to the Privacy Act, e.g., is it personally identifiable information such as name and social security number?
C	Is the information related to an EPA enforcement action and must be protected from disclosure to unauthorized personnel?
C	<p>Does the information concern law enforcement or legal activities (i.e., civil or criminal law), including the implementation of Executive Orders or regulations issued pursuant to law? If so, sensitivity applies only to the extent that an inappropriate disclosure of the information could result in the following:</p> <ul style="list-style-type: none"> - Interference with enforcement proceedings. - Deprivation of a person's right to a fair trial or an impartial adjudication. - Unwarranted invasion of the personal privacy of a living person, including surviving family members of an individual identified in such a record. - Disclosure of the identity of a confidential source, including a source within EPA, a State, local, or foreign agency or authority, or any private institution that furnished the information on a confidential basis. - Disclosure of information furnished from a confidential source and obtained by a criminal law enforcement authority in a criminal investigation, or by an agency conducting a lawful national security investigation.

**IDENTIFYING
CONFIDENTIALITY
REQUIREMENTS,**
Continued

CONFIDENTIALITY <i>(Continued)</i>	
High, <i>Continued</i>	<ul style="list-style-type: none"> - Disclosure of techniques and procedures for law enforcement investigations or prosecutions, or disclosure of guidelines for law enforcement investigations if such disclosure could be expected to risk circumvention of the law.

CONFIDENTIALITY (Continued)	
	<ul style="list-style-type: none"> Ⓒ Is the information Confidential Agency information (CAI)? Ⓒ Is the information geological or geophysical information (including maps) concerning wells?
Medium	<ul style="list-style-type: none"> Ⓒ Does the information address internal rules or practices of EPA offices that if disclosed, could adversely affect or prevent performance of Agency operations, including internal advice, recommendations or subjective evaluations? Ⓒ Does the information pertain to examination, operation, or condition reports addressing EPA's regulation or supervision of financial institutions?
None	<ul style="list-style-type: none"> Ⓒ The information is available to the public.

**4.6
TREATMENT OF
CONFIDENTIAL
INFORMATION**

EPA has specific security requirements for information where intentional, inappropriate, or accidental disclosure of the information will expose the Agency or an individual to loss or harm. Subsection 4.5 contains a list of questions that can help determine if information is confidential.

All confidential information must be accorded the following treatments:

- Ⓒ Confidential data must never be transmitted unprotected (e.g. unencrypted) via any **unsecured** information system. An unsecured information system is defined as one that has inadequate security controls. Examples of unsecured information systems include electronic mail, the Internet, Electronic Bulletin Boards and Facsimile. (Facsimile may be used to transmit confidential information only if the security of the transmission process can be assured through encryption, secured lines, or strict procedural controls.)
- Ⓒ Confidential data must not reside on information systems to be used for public access unless access controls can be guaranteed.
- Ⓒ New technologies used to provide access to or to disseminate information must ensure that confidential information is adequately protected from disclosure.

**TREATMENT OF
CONFIDENTIAL
INFORMATION,
*continued***

- C Backups containing confidential information should be adequately protected and labeled.
 - C Associate sensitivity level indicators (header/footer or other label) with computing resources, applications, and information while confidential information is being processed.
-

**4.7
HOW THE
SENSITIVITY
DETERMINATION
IS USED**

The sensitivity level and the security goals identified for the information are used for the following purposes:

- C As a means of conveying the level of importance of the information and the need to protect it. This sensitivity determination may be used by others, such as auditors and management, when conducting reviews to ensure that the information is adequately protected.
- C Within the security planning process, as a means of establishing and evaluating the necessary level of security.
- C To identify the appropriate protective techniques for the information and the application or system processing the information.

[This page intentionally blank.]

5.0 THREATS

EPA's information resources are subject to threats having the potential to prevent the Agency from meeting its obligations, including providing environmental information to the public. An awareness of the threats facing EPA's information resources is an important part of ensuring that information is available when needed, protected from unauthorized or accidental modification, and, for confidential information, protected from unauthorized disclosure.

Section 5.0 discusses the most common threats to EPA's information resources. This Section also describes the security goals that may be compromised by these threats, and standard techniques for protecting information resources.

5.1 THREAT CATEGORIES

A threat is any event or entity with the potential to cause damage to an information resource. This damage may be in the form of loss of availability, unauthorized or accidental modification of information, or unauthorized disclosure of confidential information. Common types of threats to information assets include:

- C Human error and omissions.
- C Dishonest or disgruntled employees.
- C Loss of supporting infrastructure (for example, loss of power or communications capabilities).
- C Water damage.
- C Threats from outsiders.

Figure 5-1 illustrates the percent of problems attributed to each of these threat categories.

L Note:

Viruses and hacker attacks are often portrayed as the primary area in which information resources are subject to potential loss or damage. Studies of computer-related economic losses have determined that human error and omissions are, by far, the most significant threat category. However, the threat from outside sources (e.g., hackers) has been increasing, as access to external computer resources increases.

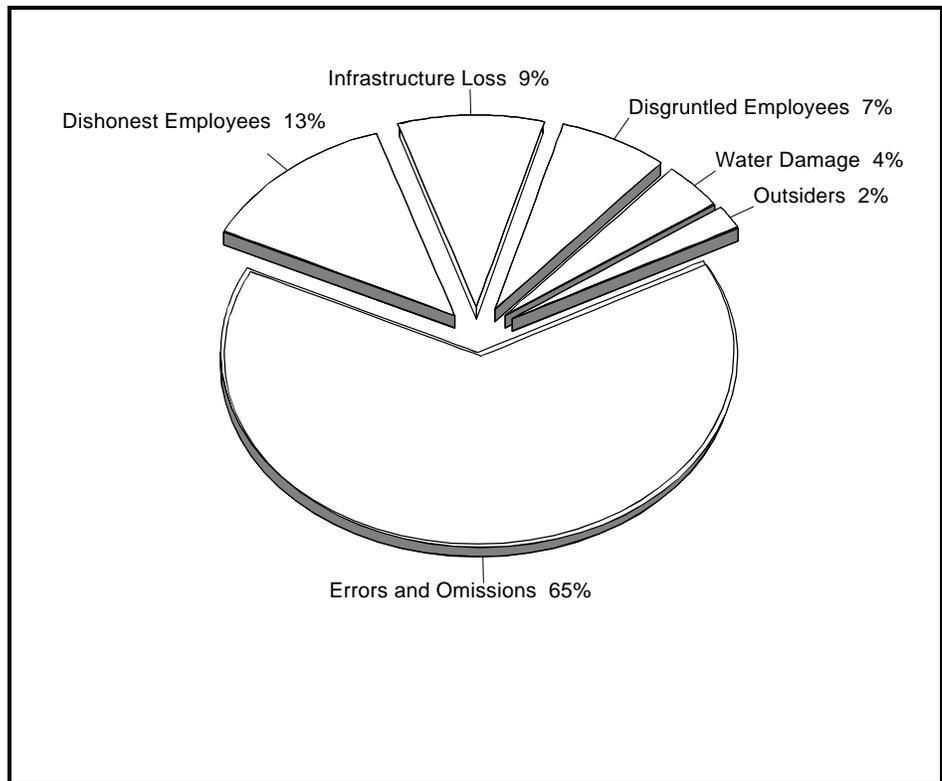
The following subsections discuss threat categories, the security goals they compromise, and standard security techniques used to protect against these threats.

Human Error and Omissions

This category represents the most frequent threat to information integrity. Invalid or inaccurate data may be introduced by data entry or editing personnel, restoring data from outdated or untested backups, or other procedures. Information may also be incorrectly modified due to programming errors. This threat category may also affect information availability and confidentiality. For example, an operator accidentally overwrites a critical file or sets incorrect file permissions allowing access to confidential information.

Controls to protect against human errors and omissions typically include data validation routines and software quality and security awareness programs.

Figure 5-1.
Percent of Problems
Attributed to
Information Threats



Dishonest or Disgruntled Employees

Dishonest or disgruntled employees represent a threat to data availability, integrity, and confidentiality if adequate controls and procedures or management supervision are inadequate. If access to information and

**Dishonest or
Disgruntled
Employees,**
Continued

information processing capabilities are not restricted, a dishonest or disgruntled employee can take advantage of this vulnerability and cause damage to Agency information resources or inappropriately disclose confidential information.

Security measures used to prevent compromise from this threat category include the following administrative and technical controls:

- C Procedures for immediately deleting access or amending permissions for terminated or transferred personnel.
- C Security awareness programs to educate supervisors, managers, and information system administrators to be alert to suspicious behavior.
- C Technical access controls to ensure that information system users are only authorized access to the information and processing capabilities required to complete their jobs.
- C System and application audit trails to record relevant information system and user activities. Note that audit trails must be regularly reviewed to identify suspicious or inappropriate activities.

**Loss of Supporting
Infrastructure**

The loss of the infrastructure that supports information processing may occur due to equipment failure, fire, loss of power or communications, or natural events, and can have a significant effect on information availability and integrity.

The primary measures taken to protect against loss of infrastructure support are environmental controls, such as fire equipment and alternate power sources. In addition, continuity of support and/or contingency plans must be developed. These plans establish the necessary procedures for continuing operations for critical systems and applications following disasters or loss of infrastructure support. The plans must be tested regularly to ensure that they remain effective.

L Note:

The terms continuity of support, disaster recovery, and contingency planning are often used interchangeably in security documentation. See Appendix A for clarification of these terms.

The following definitions are derived from Appendix III of OMB Circular A-130:

SECTION 5.0 THREATS

Loss of Supporting Infrastructure, *Continued*

- C Continuity of support plan: Documents the cost-effective steps to manage any interruption or disruption of service. Assures the ability to recover and provide the level and priority of service sufficient to meet the needs of and in consultation with the users of the system.
- C Contingency plan: Documents how the mission or function supported by and critically dependent on the major application will be performed and/or recovery from the loss of existing application support. The loss of application support can be due to the inability of the application to function or the general support system(s) failure.

Per Appendix III of OMB Circular A-130, agencies are required to prepare, document and test contingency and continuity of support plans as part of the security planning process for general support systems and major applications. Appendix A provides guidance on developing continuity of support and contingency plans.

Water Damage

As illustrated in Figure 5-1, four percent of computer problems have been attributed to water damage. This threat area typically refers to water damage resulting from water-related problems such as high humidity levels rather than from fire fighting and floods. This latter type of water damage often causes and is included in the statistics for loss of supporting infrastructure.

This threat area results in damage to equipment and media which may adversely affect information availability and, to a lesser degree, information integrity. Standard controls to protect against this type of water damage include the use of dehumidifiers and air conditioning in computer and media storage areas.

Damage from Outsiders/Hackers

Threats from outsiders, such as hackers, represent a growing risk to Agency information. Hacker attacks can result in the disruption or denial of service and compromise information integrity and confidentiality. Hackers have been known to compromise one system and to use it to gain access to more sensitive information systems. This situation may create liabilities for the owner of the compromised information system. As technology advances and the level of computer experience and understanding rises, hacker attacks become more technically challenging to protect against.

Standard controls to protect against intruders include access controls, strict

**Damage from
Outsiders/Hackers,**
Continued

access policies, implementation of firewall technologies and real time monitoring and alerts for suspicious behavior. An incident response capability to identify and limit damage when attacks are detected is critical. EPA's Computer Emergency Response Team (CERT) has been established to deal with intruder incidents. Continuity of support and contingency plans are also important in this area to recover from damages caused by intruder incidents.

**5.2
VULNERABILITIES**

A vulnerability is defined as a missing or weak security control that may allow a threat to compromise the availability, integrity, and/or confidentiality of an information system or the information it processes. An example of a common information system vulnerability is inadequate password controls. If users choose easily guessed passwords such as names, names of sports teams, or other words found in the dictionary, hackers can use software, often called a "password cracker," that can "guess" the password. Hackers can use the passwords they obtained to gain unauthorized access.

L Note:

To be cost-effective, security controls must only be used where a vulnerability exists that a threat can take advantage of, resulting in damage or unauthorized access to information systems and information. For example, a system that does not have dial-in capabilities has no vulnerabilities that a hacker can take advantage of.

**5.3
MALICIOUS
CODE: VIRUSES,
TROJAN HORSES,
AND WORMS**

Computer viruses, trojan horses, and worms, collectively referred to as malicious code, have received a great deal of attention in the press. While some of the coverage is sensational, it is clear that the problem is real and that risk does exist. The National Institute of Standards and Technology (NIST) defines viruses, Trojan Horses, and worms as follows:

C Computer virus: "program segments that copy versions of themselves into programs (targets) and thereby convert the targets into vehicles for further propagation. Viruses usually spread from program to program within a single system by reproducing every time any infected program runs. Moreover, they can spread from system to system whenever an infected program is introduced into another system."

MALICIOUS

C Trojan horse: "a program that conceals harmful code. A Trojan horse

**CODE: VIRUSES,
TROJAN HORSES,
AND WORMS,**

Continued

usually resembles an attractive or useful program that a user would wish to execute.”

- C Worm: “a self-contained program that copies versions of itself across electronically connected nodes.”

Viruses are an important area of concern for EPA because of the many applications that run on a PC platform and the common practice of sharing data and programs from these PCs via diskettes or other media. PCs do not have the same level of technical controls to protect programs and data from unauthorized modification as do larger computers. In addition, PC users often do not view virus prevention as an important concern.

**Protecting
Against Viruses**

Computer viruses are constantly changing. Follow standard virus prevention techniques. These techniques can assist in preventing compromise by viruses and include the following:

- C Use Agency-approved anti-viral software. Keep the software resident in memory, so that it will automatically scan diskettes as they are used. Anti-virus software is designed to recognize viruses based on characteristics found in virus code. As new viruses are identified, vendors update the software to recognize the characteristics of these new viruses. Therefore, user versions of the anti-virus software must be kept up-to-date to be effective.
- C Be aware of common sources of contamination—shared laptop computers, exchanged diskettes, copied or downloaded executable software, referred to as “freeware” or “shareware,” and documents containing embedded macro code (for example, MS Word documents). Occasionally, commercial software and disks used by PC or LAN maintenance personnel are sources of contamination. Use virus software to scan all media, but keep in mind that there is also a level of risk—anti-virus software may not find the newest types of viruses.
- C Follow the appropriate procedures for acquiring software. Because of the changing nature of computer viruses, it is very difficult to develop a set of generic, straightforward procedures to ensure the integrity of non-EPA or public domain software. Consequently, EPA employees must not install non-EPA or public domain software (including

“freeware” and “shareware”) on their PCs without the expressed approval of their Division Director or the Division Director's

Protecting

**Against
Viruses,
Continued**

designate.

- C Watch for unusual or suspicious program or file behavior and report it to the LAN manager or other designated contact immediately.
- C **PREPARE BACKUPS.** Until affected by a virus, many PC users are lax in ensuring that backups exist for the data and programs stored on their PCs. The frequency with which backups are made must be based on the importance of the information processed on the PC—important information and programs must be backed up at least weekly. Regular backups can help in quickly recovering from a virus incident. Be sure to test backups—ensure that the data on the backup can be restored. A schedule of backups should be established and several “generations” of backup tapes should be maintained to help ensure that files are recovered to their “pre-infected” state.

The NTSD *LAN Operating Procedures* Manual includes recommendations related to new software, backups, and regular checks for program/file size changes.

**Additional
Information**

Additional guidance on computer viruses is presented in the NIST Special Publication 500-166, entitled "Computer Viruses and Related Threats: A Management Guide." The publication, dated June 1990, provides general guidance for managing the threats of computer viruses and unauthorized use. It deals with different computing configurations such as personal computers and networks. This document, and other security-related publications, can be found on the NIST Computer Security Resource Clearinghouse web site at:

<http://csrc.nist.gov/nistpubs/sp500166.txt>

A copy is also available in the EPA Headquarters Library or through the Government Printing Office.

[This page intentionally blank.]

6.0 ROLES AND RESPONSIBILITIES

A critical component to EPA's information security program is assigning responsibility for protecting EPA's information resources. Everyone in EPA who manages, designs, programs, operates, or uses EPA information or resources has individual, job-related responsibilities that contribute toward meeting the goals and objectives of the EPA Information Security Program. This section defines specific information security responsibilities for all levels of Agency employees. These roles and responsibilities must be fully implemented within organizational security programs (see Section 12).

This Section defines roles and responsibilities for ensuring that EPA's information resources are adequately protected.

Information security roles and responsibilities are defined in the subsections below for the following EPA staff and EPA offices (Note: EPA information system users includes EPA contractors and grantees):

- C Primary Organization Heads.
 - Deputy Administrator (DA).
 - Assistant Administrator (AA).
 - Regional Administrator (RA).
 - Chief Financial Officer (CFO).
 - Inspector General (IG).
 - General Counsel (GC).
- C Office Directors (OD).
- C Division Directors (DD).
- C Senior Information Resources Management Officials (SIRMOs).
- C Information Security Officers (ISOs).
- C EPA Information Managers.
- C EPA Information System Users (includes EPA employees, contractors, and grantees).
- C Office of Acquisition Management (OAM).
- C Office of Grants and Debarment (OGD).
- C Office of Environmental Information (OEI).
- C Facilities Management and Services Division (FMSSD).
- C Office of Inspector General (OIG).
- C Office of the Chief Financial Officer (OCFO).
- C Project Officers, Delivery Order Project Officers, and Work Assignment Managers.
- C EPA managers and supervisors.

In instances where security issues are raised by the AAs, the Chief Information Officer (CIO) has the final decision authority.

SECTION 6.0 ROLES AND RESPONSIBILITIES

6.1 Primary Organization Heads

Primary Organization Heads to include the Deputy Administrator, Assistant Administrator, Regional Administrators, the Chief Financial Officer, the Inspector General, and the General Counsel. Each Primary Organization Head shall:

- C Establish an organization-wide information security program to include laboratories and other facilities that is consistent with the organizational mission, the ISM, and other Agency policies. 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.
- C Ensure the adequate protection of information, general support systems, and applications belonging to or maintained by the organization based, in part, on the security plan and periodic reviews and/or audits.
- C Ensure that responsibility for the security of general support systems and major applications is assigned in writing to personnel with the appropriate skills (Per Appendix III, OMB Circular A-130).
- C Ensure that appropriate safeguards are incorporated into all new organizational information systems and major modifications to existing systems.
- C Ensure 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 significant change occurs.
- C Ensure that a SIRMO is designated, who is knowledgeable in information technology and security, to be responsible for the security and management of all information systems in the organization.
- C Designate ISO(s), in writing to the Chief Information Officer (CIO), Office of Environmental Information (OEI) with a background in information technology and security, to be responsible for ensuring the comprehensiveness of their security program and the security of their information assets.

Primary Organization Heads,

- C Ensure that the National Information Security Program is notified of any deletion of an ISO.

Continued

- C Ensure that written authorizations to operate, signed within their organizations, factor in the results of the most recent review or audit of controls for major applications, and an assessment of management, operational, and technical controls or the most recent review of controls for general support systems.
- C Provide annual written certification to the EPA Chief Information Officer (CIO) that security plans (1) are in place and current for each general support system and major application within the organization and (2) provide adequate security of the organization's information resources in accordance with Federal and Agency policy.
- C Ensure that deficiency determinations pursuant to OMB Circular A-123, "Management Accountability and Control," consider the controls listed in Appendix III of OMB Circular A-130 for general support systems and major applications within their organization (i.e., written assignments of responsibility for security, security plans, and written authorizations for processing or use).
- C Ensure the continuity of operations of automated information systems and facilities that support critical functions and organization mission.
- C Ensure that Federal employees and contractor personnel understand their information security responsibilities, and that organizational information security regulations are properly distributed.
- C Ensure that all organizational procurements of Automated Data Processing (ADP) equipment, software, and services incorporate adequate information security provisions.
- C Ensure that the Information Security Program established by the Primary Organization Head in their organization fully implements the Agency's information security policies.

6.2 Office Directors

Office Directors (OD) shall:

- C Ensure that the Information Security Program established by the

SECTION 6.0 ROLES AND RESPONSIBILITIES

Primary Organization Head in their organization is fully implemented.

- C Ensure that the office's Information Security Program meets FMFIA reporting requirements.

6.3 Division Directors

Division Directors (DD) shall:

- C Ensure that responsibility for the security of general support systems and major applications is assigned in writing to personnel with the appropriate skills (Per Appendix III, OMB Circular A-130).
- C Ensure that all general support systems and major applications have a written authorization to process based on an evaluation of their security plan.
- C Ensure that major applications, within the organization that promote or permit public access, only allow access to appropriate types of information. Provide authorization in writing before the major application is made accessible to the public.
- C Ensure that EPA employees do not install non-EPA or public domain software (including "freeware" and "shareware") on their PCs without approval.

6.4 Senior Information Resources Management Officials (SIRMOs)

SIRMOs shall:

- C Be responsible to the Primary Organization Head for EPA information security implementation, ensuring that information security requirements are satisfied for information systems within the organization.
- C Evaluate whether a comprehensive information security program is implemented within the organization.
- C Ensure that all organizational procurements of ADP equipment, software, and services incorporate adequate information security provisions.

Senior Information Resources Management Officials (SIRMOs)

- C Approve general support system and major application security plans. Ensure, at least every three years, that all automated information systems in their primary organization meet the information security planning requirements of the ISM.

Continued

- C Ensure that manual information systems within the organization provide security for information at least equivalent to the security afforded by computer-based information systems that handle the same information.

**6.5
Information
Security Officers
(ISOs)**

The primary role of an ISO is to ascertain that a current information security program is in place for his/her respective organization and that the information is properly managed from an information security perspective. The ISO provides the SIRMOMO with adequate information to determine the effectiveness and appropriateness of information security practices for information systems under their purview. In this capacity, ISOs take on the following responsibilities:

- C Coordinate information security activities with the individuals (e.g., PC Site Coordinators, LAN Administrators, and information managers) who are directly responsible for implementing the practices and safeguards defined in their organizational information security program.
- C Provide the guidance and documentation necessary to enable security plan developers to complete their security planning responsibilities.
- C Verify and review specifications for the acquisition or operation of the organization's information technology resources, regardless of acquisition method, to determine if appropriate technical, administrative, physical, and personnel security requirements are included.
- C Review security practices within the organization to help ensure that appropriate levels of information security are maintained.
- C Ensure that appropriate individuals within the organization are cognizant of their responsibilities to develop security plans and to update them at least every three years. Maintain a file containing copies of the organization's current and completed security plans. Ensure that each completed security plan contains the signatures of a SIRMOMO and the responsible managing official authorizing operation.

ISOs, Continued

- C Ensure that responsible individuals within the organization are cognizant of the need for background screening for personnel who have the ability to override technical controls or who have access to information or information systems which warrant an individual's screening prior to access.

- C Ensure that all personnel involved in the management, use, or operation of information systems receive training in methods to protect information, and are aware of potential threats and vulnerabilities.
- C Verify that physical security requirements have been fulfilled for the organization as stipulated by the NTSD Operational Directives and FMSD requirements identified in EPA Directive 4800, *Facilities and Support Security Manual*.
- C Ensure that responsible individuals throughout the organization are cognizant that security requirements must be considered throughout the acquisition, development, and operation of computer applications, including commercial-off-the-shelf software.
- C Ensure that when a breach in information security occurs, appropriate personnel and offices (such as the SIRMO, EPA CERT, OIG, and information owners and stewards) are notified, and that corrective actions are documented.
- C Keep DDs and ODs apprised of when security plans require revision.

**6.6
Information
Managers**

Information Managers can be information owners, information stewards, or EPA support system or application managers/stewards or information system sponsors. An information manager may be responsible for more than one information system, general support system or major application. To fulfill their responsibilities, information managers must interact with the managers responsible for the applications and systems on which the information resides (information stewards). For example, an information manager responsible for completing a security plan for a major application operating on EPA's mainframe, must contact the NTSD security staff at the National Computer Center (NCC) to obtain a copy of the mainframe's security plan, and ensure that the major application security plan is reviewed by that NCC manager (the responsible primary system manager), from an information security perspective.

**Information
Managers,
Continued**

The information manager shall:

- C Develop and document automated information system security requirements and specifications.
- C Develop and maintain information system documentation for inclusion in the Information Systems Inventory (ISI) and in the security planning

process.

- C Plan and perform automated information system security specification tests.
- C Determine and implement required changes resulting from the tests of the information systems design.
- C Designate sensitivity levels for information in accordance with the Sensitive Information Criteria in the *ISM* (Section 4 of this Manual).
- C Develop security plans for manual and automated information systems.
- C Implement and monitor the Information System Security Plan.
- C Contact the organization's ISO for the purpose of conducting periodic reviews of security controls and of completed security plans.
- C Evaluate information security violations, variations, and incidents and report recommended actions to the ISO.
- C Ensure that users are informed of their information security responsibilities.
- C Ensure that appropriate safeguards are built into new information systems and during major modifications to existing systems.
- C Ensure that controls, for applications and/or systems for which they are responsible, are periodically reviewed or audited in accordance with Federal and EPA requirements.
- C Ensure that organizational security regulations are properly distributed.
- C Ensure that software and hardware documentation is maintained appropriately. This includes information system manuals, user guides, and license agreements for commercial off-the-shelf hardware and software.
- C Ensure that all personnel are complying with software licensing agreements.
- C Ensure that only authorized personnel access Agency information.

**Information
Managers,
*Continued***

- C Ensure that information systems are reviewed in accordance with EPA and Federal policy (independent advice and comment of general support systems and review of major applications by primary general support system owners).

**6.7
EPA Information/
Information System
Users**

EPA information system users include **EPA employees and agents, including contractors and grantees**. Each information system user shall:

- C Fulfill assigned information security responsibilities.
- C Attend required information security awareness training and attend specialized information security training as appropriate.
- C Limit access only to information and information systems to which he or she is authorized access.
- C Adhere to all Agency and organizational information security policies, standards, and procedures.
- C Report information security violations to the information manager of the information system and to the Computer Emergency Response Team (CERT) or other designated official, as required by security plans, grant agreement or contract terms. In addition, report violations involving NSI to FMSD and the Inspector General and, if applicable, the Contracting Officer. See Appendix E for point of contact.

**6.8
Office of Acquisition
Management
(OAM)**

The Office of Acquisition Management (OAM) shall:

- C Ensure that Agency contract policies, solicitations, and award documents contain provisions (as promulgated by OEI) specifying information security responsibilities of contractors.
- C Ensure contracting officers adequately address and include specific information security requirements, identified in Statements of Work, in the terms of the contract.
- C Establish procedures to monitor contractor compliance with information security responsibilities as specified in Agency contracts.

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.

- C Include appropriate provisions/clauses, regarding information security and disclosure of confidential information to contractors, in contracts and ensure contracts comply with disclosure requirements stipulated in 40 CFR 2 (Public Information).

**6.9
Office of Grants and
Debarment (OGD)**

The Office of Grants and Debarment shall:

- C Ensure that Agency grant and interagency agreement policies, solicitations, and award documents contain provisions (that have been promulgated by OEI) concerning the information security responsibilities of interagency contractors and grantees that access or handle EPA information or information systems.
- C Establish procedures to ensure that interagency contractors (and grantees accessing or handling 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.

**6.10
Office of
Environmental
Information (OEI)**

OEI shall:

- C Develop and define an Agency information security program in accordance with applicable Federal laws, regulations, and executive orders.
- C Ensure that all Agency organizations are aware of their compliance responsibilities as they relate to the Agency's Information Security Program.
- C Provide guidance on selecting and implementing safeguards for information systems.

SECTION 6.0 ROLES AND RESPONSIBILITIES

- C Establish security awareness training criteria.
- C Develop, implement, and supervise the physical security of the computer processing areas at the NCC in Research Triangle Park, North Carolina; and the Washington Information Center (EPA HQ).
- C Establish the minimum information security control environment required for the Agency to protect both its ADP resources and its information from theft, damage, and unauthorized use.
- C Establish and implement the minimum security controls for EPA's network connectivity (including Internet connectivity) required for the Agency.
- C Ensure that EPA's LANs comply with Agency standards for LAN information security.
- C Report all information security violations and recommendations for corrective action in writing to the designated information manager and to the NCC Security Officer.
- C Develop and maintain the Agency's CERT capability.

6.11 Facilities Management and Services Division (FMSD)

FMSD shall:

- C Establish and implement physical security standards, guidelines, procedures, and controls in accordance with EPA information security and applicable physical security policies.
- C Establish and implement standards and procedures for NSI in accordance with EPA Information Security Policy and all applicable Federal laws, regulations, and executive orders.

6.12 Office of Inspector General (OIG)

OIG shall:

- C Establish 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.

- C Review allegations of waste, abuse, mismanagement, or criminal activity involving information security.

**6.13
Project Officers,
Delivery Order
Project Officers, and
Work Assignment
Managers**

Each Project Officer (PO), Delivery Order Project Officer (DOPO), and Work Assignment Manager (WAM) shall:

- C Ensuring that contractor personnel are aware of their information security responsibilities.
- C Ensure 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.
- C Ensure that appropriate contract, grant, or interagency agreement personnel and the appropriate level of required background screening are identified in acquisition documents when access to EPA information or information systems is required.
- C Ensure that the appropriate level of background screening is performed.

**Project Officers,
Delivery Order
Project Officers, and
Work Assignment
Managers,
*Continued***

- C Ensure that specific information security requirements are identified in acquisition documents.
- C Ensure that mechanisms and controls to enable access and communications, such as user IDs and mailing lists, for acquisition personnel are established, accurate, and current to prevent unauthorized or unnecessary access to or disclosure of information.

**6.14
EPA Managers and
Supervisors**

Each EPA manager and supervisor shall:

- C Ensure subordinates are made aware of their information security responsibilities and receive necessary and required training.

SECTION 6.0 ROLES AND RESPONSIBILITIES

- C Ensure subordinates adhere to the organizational information security program established by the appropriate Primary Organization Head.
- C Ensure information security violations are reported to the appropriate ISO and information manager.
- C Ensure subordinates are compliant with software licensing agreements.

7.0 INTERNET USE

The Internet is a popular medium for viewing and publishing information because it provides easy access to diverse collections of information. While the Internet serves as a gateway to large amounts of information, it may also place EPA information resources at risk. In addition, because the Internet provides access to both “valuable” and “not so valuable” information, EPA must ensure that its Internet resources are being used wisely and to the benefit of the Agency and the public.

This Section discusses Internet security requirements. The Section includes a discussion of the risks in the Internet environment, secure use of the Internet, and appropriate use of EPA’s Internet resources.

This section focuses on Internet security issues and appropriate use of EPA’s Internet resources from the perspective of a “web user”—someone who uses the Internet to search for and gather data. See Section 8, Public Access Information Systems, for security issues and requirements for Internet publishers.

This section does not address detailed, technical requirements for establishing secure Internet connections. For further information on technical Internet issues, contact the NTSD security staff.

7.1 RISKS IN THE INTERNET ENVIRONMENT

The Internet, like any automated processing environment, is subject to risks that can lead to the compromise of information resources. However, the very aspect of the Internet that makes it popular—easy (and anonymous) access to computers providing information in electronic form—also poses risks to those using the Internet. Internet risks include the following:

- C **Eavesdropping.** Eavesdropping (i.e., reading data as it crosses the network) can occur because network protocols broadcast data in clear text. Many information systems also broadcast passwords in clear text. Software is available that can monitor and capture network traffic.
- C **Spoofing (also referred to as impersonation).** Most Internet traffic is unencrypted. Therefore, passwords, E-mail, files, etc., can be monitored. Hackers can peruse Internet traffic and capture login information, such as passwords and account numbers. Web browser software can be set up such that the user can “look like” someone else. This information can be used to impersonate legitimate users and gain access to the site’s computer.
- C **Data manipulation.** Data can be captured and modified or rerouted as it is routed through various Internet sites.

RISKS IN THE INTERNET

ENVIRONMENT,
Continued

- C **Hacking.** Many systems providing Internet services are not adequately configured for security or do not contain the latest security patches to the operating system. Site administrators may not be aware of security problems in hardware and software and have not installed the necessary patches. In addition, many computer information systems are shipped and installed with poor default security configurations. Compounding the problem is the fact that network personnel often do not have the authority to implement the appropriate security measures such as firewalls.

 - C **Viruses.** The Internet provides an opportune environment for the exchange of computer viruses. "Shareware," i.e., free software, is readily available on the Internet. However, downloading virus-infected executables or trojan-horse programs can result in significant losses from damaged information systems and destroyed data.
-

7.2
USING THE
INTERNET
SECURELY

While there will always be risks in the Internet environment, there are ways to reduce these risks to an acceptable level. The following is a list of required activities for reducing the risks of Internet use:

- C To protect the availability of the information system, ensure that software is obtained from reputable sources. Avoid the use of shareware and alpha or beta test versions of software. If the use of shareware is necessary, test the software on an isolated machine.

- C Do not download unapproved software, including browsers, applets, and viewers.

- C Scan for viruses on a regular basis using EPA-approved anti-viral software.

- C Backup data and programs at least weekly. Test backups to ensure that recovery is possible if the information system is damaged by software containing "bugs" or computer viruses.

USING THE
INTERNET
SECURELY,

- C Assess the sensitivity of the information before processing or transmitting over the network. Confidential data must never be transmitted across an unsecured medium such as the Internet unless

Continued

encrypted.

- C If message integrity is critical, use MACs (message authentication codes), digital signature technologies or other acceptable means. These mechanisms can be used to determine if the contents of a message were altered during transmission. The NIST web site provides detailed information on the use of MACs and digital signatures. The URL for NIST Federal Information Processing Standards on computer security is: <http://csrc.nist.gov/fips/>
- C System Managers must remain apprised of and current on operating system vulnerabilities. Subscribing to services that provide alerts on these vulnerabilities is the most effective means. Test and install patches as soon as possible.
- C If developing or operating an Internet site or otherwise posting information to the Internet, review the requirements presented in Section 8, Public Access.

7.3 APPROPRIATE USE OF THE INTERNET

The Internet can enhance productivity by providing EPA staff with ready access to large amounts of valuable information. In addition, the Internet provides a popular medium for the Agency to use in making information available for public access. However, because the Internet provides access to such diverse information, the temptation to use the Internet for other than authorized purposes may be strong.

As with all of EPA's information resources, Internet connectivity is paid for by the Government using taxpayer dollars. Therefore, the Agency must ensure that this money is spent wisely. EPA's policy for the appropriate use of the Internet is the same as for all its information resources:

- C Information technology resources are to be used for authorized purposes only.
- C The use of EPA information technology resources for unauthorized personal business is not allowed.

Appropriate Internet Activities

Appropriate Internet activities include the following:

- C **Browsing and Searching**

Browsing and searching for the following types of information or information sources:

- Directly related to official duties.
- Associated with education or training paid for or sponsored by EPA.
- Needed to maintain user's EPA work-related skills or a dual professional classification as provided for in EPA personnel management policies and guidelines.

C Sending and Receiving Electronic Messages or Files

Using the Internet to send and receive electronic messages and files is appropriate under the following conditions:

- All messages and files must be for authorized use.
- Transmitted information and files must not violate copyright laws or licensing agreements.
- Confidential information must not be transmitted unless adequately protected (i.e., encrypted).
- Message attachments and files (e.g., executables and documents containing embedded macro code) must be scanned for viruses both prior to transmission and after receipt.

L Note:

If a records disposition schedule does not exist for E-mail messages, these messages may be considered part of the public record.

**APPROPRIATE USE
OF THE INTERNET,**
Continued

C Accessing news groups; distribution and mailing lists; and Usenet groups

Accessing news groups; distribution and mailing lists; and Usenet groups is appropriate under the same conditions specified for browsing

and searching. Note: EPA employees must use a disclaimer unless authorized to represent an official EPA position.

L Note:

The use of “chat rooms” or online forums is generally inappropriate unless officially sanctioned or approved by management.

7.4 PENALTIES FOR INAPPROPRIATE USE

Agency information resources must not be used for unethical, malicious, or illegal activities or in a manner that constitutes a waste or abuse of government resources. Employees who use EPA’s information resources, including access to the Internet, for other than authorized use are subject to disciplinary action. Depending on the severity of the violation, at the discretion of management and through due process of the law, disciplinary action may range from reprimand to dismissal, and may include criminal or civil penalties.

Copyright Issues

When gathering information from Internet sources, it is important to be aware of copyright issues. A common misconception is that all information published on the Internet is in the public domain and is therefore free. As with software, because information is publicly available doesn’t necessarily mean that it isn’t copyrighted. There are many Internet sites discussing the copyright issue as it pertains to information published electronically. The following is a brief list of sites providing an overview of copyright requirements:

<http://www.clari.net/brad/copymyths.html>

<http://publications.urel.wsu.edu:80/Copyright/Copyright.html>

<http://www.fplc.edu/tfield/cOpyNet.htm>

[This page intentionally blank.]

8.0 PUBLIC ACCESS

EPA's mission includes providing environmental information to businesses, state and local governments, communities, and citizens. The Agency provides access to a large volume of environmental information through information systems made widely available to the general public. In addition, EPA is mandated by law and regulation to provide electronic access to certain categories of Agency information.

Information provided to the public must be accurate,

protected from accidental or unauthorized modification, and available when requested. In addition, the Agency must ensure that information not appropriate for public release is not accidentally or intentionally disclosed.

This Section discusses public access information systems, their potential influence on public perception, security issues, mandated security requirements, and the security procedures necessary to adequately protect public access information systems.

8.1 PUBLIC PERCEPTION

Providing quick and easy access to high-quality environmental information is a key factor in the confidence that the public and EPA's partners have in the Agency. Conversely, problems with public access information systems can undermine the public's confidence in EPA. These problems can include:

- C Providing access to inaccurate information or information that has been accidentally or intentionally modified.
- C Frequent or prolonged unavailability of public access information systems.
- C Violating the privacy of public access information system users.
- C Sharing software containing viruses or trojan horses.

Public access information system owners and managers must evaluate the security issues facing their information systems and implement the appropriate procedures to ensure that these problems do not adversely affect the Agency's information dissemination efforts.

8.2 SECURITY ISSUES

Security issues in the public access environment include:

- C Hacker activity.
- C Compromise of confidential information.

SECURITY ISSUES,
Continued

- C Accidental or malicious modification of data.
- C Loss of system processing support.
- C Computer viruses.

These five issues are discussed below.

Hacker Activity. Public access systems are key targets for hackers—the systems are easily accessible, often well advertised, and usually do not require an account in order to access the system. Hackers, or even disgruntled employees, may break into the system in an attempt to discredit the Agency. If the computer system is not configured correctly, system access controls may be circumvented and a hacker may gain access to system files and, therefore, control over the computer system.

L Note:

The U.S. Department of Energy (DOE) Computer Incident Advisory Capability (CIAC) lists many vulnerabilities that, if not addressed, could be exploited to gain control of information system resources. CIAC Bulletins are available through the Internet at the following address:

<http://ciac.llnl.gov/cgi-bin/index/bulletins>

Compromise of confidential information. If confidential information is stored or processed on a information system providing public access services, the possibility exists for access controls to be circumvented and the confidentiality of the data to be compromised.

Accidental or malicious modification of data. If access is not appropriately controlled, data stored on the computer may be accidentally or intentionally modified.

Loss of system processing support. Threats such as hacker activity, viruses, equipment malfunction, etc. can lead to system failure and denial of service.

Computer viruses. If system users are allowed to upload or download executable code then it is possible for users to inadvertently infect the system. If the system is infected, then software intended for public distribution may also be infected.

**8.3
MANDATED
REQUIREMENTS
FOR MAJOR
APPLICATIONS**

Appendix III of OMB Circular A-130 sets forth several requirements for major applications that provide access to the public. The Circular states that agencies must implement additional controls for these applications to “protect the integrity of the application and the confidence the public has in the application.” Controls are to include segregating official Agency records from information that is made directly accessible to the public; providing training; and documenting controls in the major application’s security plan.

L Note:

Training is required for all users of major applications, even public access information systems. For a public access information system, training may be a notification at the time of access that lists users’ responsibilities and rules for use.

The major application security plan must document application vulnerabilities and the controls used to protect the public access application. For additional information on security planning, refer to the EPA *Information Security Planning Guidance* document.

**8.4
PROTECTING
PUBLIC ACCESS
INFORMATION
SYSTEMS**

To protect Agency public access information systems and ensure data integrity, quality, and continuity of operation, evaluate the vulnerabilities and threats facing the application and system. Implement the necessary technical and procedural security controls, including the following:

- C Use a dedicated information system for public access unless approved by the CIO. Any information on the server may be disclosed if the server’s access controls are compromised.
- C Segregate official Agency records and confidential data from data intended for public access.
- C Implement access controls to ensure that a malicious user cannot break through information system controls and modify data intended for public access; steal or copy confidential data (including password files); or take control of the computer.

**PROTECTING
PUBLIC ACCESS
INFORMATION
SYSTEMS,**
Continued

- C Do not provide access to “live” Agency data. NIST recommends that agencies generate a copy of databases to be used for public access. The public must be informed of date and time the data was posted or uploaded and how often the data will be updated.
- C Ensure plans are developed and tested for each of the following areas:
 - Backups
 - Continuity of support
 - Contingency
- C Implement audit controls or real time detection software to detect intruder activity.
- C Conduct periodic security reviews to ensure that technical security controls are installed and functioning as intended. A common vulnerability is the implementation of information systems with their security controls in a default or “turned off” mode and default accounts with default passwords. While system software for most computers has built-in security controls, the equipment is often shipped and installed using the default system configuration in which the security controls are turned off. In the Internet arena, this vulnerability is frequently exploited.
- C Regularly scan the system for viruses, especially software intended for public use.
- C Develop information posting procedures. Procedures must address the following issues:
 - Which information is appropriate and not appropriate for public access.
 - How information will be initially reviewed and periodically re-reviewed to ensure its accuracy.

**PROTECTING
PUBLIC ACCESS
INFORMATION
SYSTEMS,**
Continued

- How often posted information will be updated and how the public will be notified of its currency.
 - Who will review information to ensure that information that may embarrass the Agency is not inadvertently posted on the information system.
-

**8.5
PRIVACY
CONCERNS**

Privacy concerns must be taken into account for public access information systems. While information gathered in the operation of a public access information system may not necessarily include Privacy Act data as defined by Public Law 93-579, it may still be considered “private”—few people want their name or E-mail address published for everyone to see. Not respecting the privacy of users who access public sites by allowing access to their e-mail addresses, user names, or phone numbers may undermine the credibility that the public places in the organization’s site. Consider the following privacy issues when designing and operating public access information systems:

- C Audit software may record the E-mail address of persons accessing the information system. Use audit information only as a means of detecting intruder activity.
- C If the information system gathers user information for contact or mailing purposes, maintain the privacy of the information gathered—do not share the information with other sites, agencies, etc.
- C When publishing Agency contact information, list the organization as the point of contact. This will lessen privacy concerns as well as make it more likely that information will not require updating should the person serving as the point of contact change positions.

[This page intentionally blank.]

9.0 FLEXIPLACE

Flexiplace is an alternative work-place solution that can ease traffic congestion, save energy, and assist in meeting air quality goals. Many EPA employees use flexiplace, both short- and long-term, as an alternative working arrangement. For the purposes of this document, flexiplace is defined as using an alternative work location to access EPA systems in order to complete assigned tasks. A common flexiplace arrangement is one in which an EPA employee works out of his/her home. An alternate work site may also be an office setting, such as a satellite office or telecommuting center. The function of these alternative work sites is to provide EPA personnel with remote access to Agency information and computer services. While flexiplace provides many benefits, the remote work environment adds an element of risk for EPA information resources. This section discusses security concerns in the flexiplace environment and standard security measures that must be established to ensure that Agency information resources are adequately protected.

The Agency's flexiplace policy promotes working from outside the standard office environment. Flexiplace can ease traffic congestion, save energy, and help reduce air pollution. However, providing remote sites with access to EPA information may place EPA's information resources at risk. This Section discusses security concerns in the flexiplace environment and presents procedures for securing the alternate work site to ensure that Agency resources are adequately protected.

9.1 SECURITY CONCERNS:

Because a flexiplace environment requires a remote connection to an EPA system, the connection is vulnerable to the risks inherent in remote access, including the following:

- | | |
|---|---|
| T Remote Access | C Confidential information, such as CBI data and even network passwords, can be viewed (electronically intercepted) if transmitted in plain text. |
| T Unsecured Processing Environment | C Availability can be compromised through denial of service attacks using information gained by monitoring remote network traffic (e.g., passwords and user accounts). |
| | C Integrity can be compromised if data is captured and modified while in transit. |

In addition, especially in the work-at-home environment, Agency information, hardware, and software are removed from a normal, central office or computer processing center. The information, hardware, and software face threats inherent to any processing environment. Food, smoke, heat, and excess moisture can damage equipment and removable media, and viruses can corrupt software and data. In the work-at-home

SECURITY CONCERNS,
Continued

environment, even family members can pose a threat to Agency information. If the PC is used by family members for other activities, data and software can accidentally be viewed, copied, modified, or even deleted.

When using an alternate work site, EPA employees must be cognizant of day-to-day activities that can affect security. Employees must follow standard security procedures to ensure that the Agency's information, hardware, and software are adequately protected. The following sections discuss security procedures for the flexiplace environment.

9.2 SECURING THE FLEXIPLACE ENVIRONMENT:

This section discusses security procedures from the employee's point-of-view, that is, the practices that the employee must follow in the flexiplace environment to ensure that Agency information resources are protected.

- T Protecting Agency Information**
- T Protecting EPA Hardware and Software**

In any information processing environment there are standard security practices that each employee must follow. Note that these practices alone will not ensure that information accessed remotely is secure. The information and information system manager must also establish the appropriate security measures for the remote information and information system to be accessed. This section lists the required controls for the flexiplace environment.

- C** Complete general support system and, where appropriate, application training. Be well-versed in the rules of the support system and major application. These rules define what behavior is acceptable when using the Agency's general support systems and major applications.
- C** Complete periodic security awareness training. When working alone, such as from home, security awareness training is especially important. Users must understand what can pose a threat to the information system and the procedures they must follow to protect the availability, integrity, and, if applicable, the confidentiality of Agency information.
- C** In instances where confidential document removal is necessary, official management approval must be obtained. Management must be satisfied that the organization's requirements for securing confidential information will be met.

SECURING THE FLEXIPLACE

- C** Learn to recognize signs that the system has been affected by a virus or that someone is trying to gain access to the information system

ENVIRONMENT,
Continued

remotely. Report suspicious activity immediately. Keep the necessary phone numbers easily accessible.

- C Follow all personnel and software agreements related to the flexiplace environment, including use of confidential data and copyrights and licensing agreements.
- C Ensure that the computer and remote access capabilities (modems, lines, etc.) provided by EPA are used for authorized activities only.
- C Realize that users are responsible for their own actions while using Agency-supplied information and accessing EPA information systems. Accountability is based on the user's connection, account, and password, and where applicable, the user's signature used to obtain Agency information resources.
- C Protect passwords. Follow system or application standards when choosing a password. Do not embed a password in email messages or files where they appear in plaintext. Do not share passwords.
- C Protect equipment and media (diskettes, papers, etc.) from damage. Do not eat, drink, or smoke around computers or media. Install a smoke detector. Ensure that the remote office area is not subject to excess moisture (i.e., a damp basement) or flooding. Use a surge protector.
- C Follow standard Agency virus protection procedures. Do not load unauthorized software on equipment. Use Agency-approved anti-virus software to scan all diskettes and remote files for viruses before accessing them. Scan the hard drive daily.
- C Backup software and data. Unlike the Agency mainframe and LAN environment where data is automatically backed up for users, in the remote office users must ensure that they have backups. Backups will be critical if systems are infected by a virus, lose power, or have a hardware or software failure.

**SECURING THE
FLEXIPLACE**

- C Do not transmit confidential data across any unsecured medium—by facsimile, Internet, or other unsecured network. Control access to printers at the flexiplace location, if used to print confidential data.

ENVIRONMENT,
Continued

- C Do not place other Agency information and applications at risk by trying to access resources that you are not authorized to access.
-

9.3
SECURING THE
REMOTE ACCESS
INFORMATION
SYSTEM

This section discusses security requirements and procedures from the information/information system manager point of view. These are the procedures that the information/information system manager must follow to ensure that a remote connection is acceptable and can be adequately secured.

As with any processing site, care must be taken to ensure all threats and vulnerabilities are identified and adequate controls are implemented. Consideration must be given to the threats and vulnerabilities unique to specific flexiplace environments, because it is unlikely that any two environments will be identical. Identifying security requirements for flexiplace environments is critical to ensuring that the risk introduced by remote access is maintained at an acceptable level.

Before allowing remote connections ensure that the following activities have been completed:

- C Identify the type(s) of information to be processed and its availability, integrity, and confidentiality concerns. For example, is the data to be accessed CBI? Is it financial data?

L Note:

If information, when shared, can't be provided with the same level of security that it was provided while in its native environment, then the information must not be downloaded to or shared with another computer.

- C Determine which information system(s) will be accessed and the level and type of access required, i.e., access to which applications, files, utilities, etc. Does the worker need to share files with other employees? Define the level of access to be allowed based on the job responsibilities of the flexiplace worker.

SECURING THE
REMOTE ACCESS
INFORMATION
SYSTEM, Continued

- C Complete a risk assessment. Identify the threats, vulnerabilities, and necessary safeguards to adequately protect a remote connection to the system and any applications. What are the vulnerabilities of the method in which data will be accessed, i.e., will information be

transferred across the Internet? Include in the assessment the threats and vulnerabilities in the flexiplace environment. Is the flexiplace environment a shared work space with other organizations? Is it an employee's home? If so, does the employee understand the security implications of dial-in connections?

- C Ensure that rules of behavior specific to remote access requirements have been developed for the remote support system and application.
- C Ensure that training and a security awareness program are developed for system and application users in a media and/or format that is appropriate for the flexiplace environment. For example, the use of computer-based training (CBT) courses and hardcopy manuals, rather than just lectures and briefings.
- C Ensure that training is provided prior to allowing remote access. Training must cover the risks of the remote connection.
- C Update the support system (and application, if an application will be accessed remotely) security plan. Ensure the risk assessment results are incorporated into the security plan.

[This page intentionally blank.]

10.0 PERSONNEL SECURITY AND TRAINING

EPA's employees are the Agency's key resource in its endeavor to protect the Agency's information and information systems. However, employees can also be one of the weakest links in an information security program; statistics show that up to 65 percent of computer problems, from errors to intentional damage, are caused by insiders. To ensure that EPA can rely on its personnel to protect the information and information resources entrusted to them, EPA must ensure that basic personnel security controls are implemented and practiced in each Office and Region. Personnel security controls include the following:

*EPA depends on its personnel to ensure that the information resources in their care are adequately protected. This Section describes the minimum requirements for personnel security within the Agency, including personnel screening procedures, **information system access administration, separation of duties, and security awareness and training.***

- C Personnel Screening for EPA Contractors.
- C Information System Access Administration.
- C Separation of Duties.
- C Security Awareness and Training.

The following subsections explain the controls listed above and describe their application within the Agency.

10.1 PERSONNEL SCREENING

This subsection presents personnel screening procedures. Some organizations may already have screening procedures in place due to the sensitive nature of their information. Organizational screening procedures may be more stringent than the procedures presented in this section, but all personnel screening procedures must meet the minimum screening requirements set forth below.

L Note:

The following screening requirements are directed at contractor personnel on the basis that their Federal counterparts are screened during the hiring process. For Federal employees requiring a higher level of screening, contact the Chief, Personnel Security Staff, in the OIG.

Minimum Personnel Screening Requirements PERSONNEL

Screening is required for contractor personnel in the following categories:

- C Contractor personnel who are authorized to bypass significant technical and operational security controls of an information system must be screened. **Contractor LAN administrators must be screened.**

SCREENING,
Continued

- C Contractor personnel with authorized involvement in major applications.
- C Contractor personnel with authorized access to confidential information.

The minimum level of screening is a National Agency Check with Inquiries and Credit (NACIC). Screening is conducted by the Office of Personnel Management (OPM).

The contractor screening requirement does not apply to LAN managers because **LAN managers must be EPA employees.**

L Note:

Because the potential risks vary from organization to organization, EPA managers must determine if contractor personnel require a higher level of screening. The minimum level of screening must be equal to their Federal counterparts.

Forms required for conducting the screening will be provided to contractor personnel, through their respective contract administration personnel (PO, DOPO, WAM, etc.) by NCC security staff. Instructions for completing the forms will also be provided. Completed forms are to be returned to NCC security staff for review and processing by the Office of Personnel Management (OPM). Each organization is responsible for funding the screening (whoever has the need, pays for the screening).

A NACIC takes approximately 65 days. Results of the screening are returned to EPA through the OIG for adjudication. The OIG will provide the results to the NCC security staff. Favorable screening results will be returned to the respective contract administration personnel. If the results are unfavorable, NCC security staff will coordinate with the Contracting Officer (CO), the OIG, and the contractor organization for any additional action which may be required.

The NACIC screening must occur prior to providing contractor personnel with access to EPA systems. Contractor personnel must submit required background investigation documentation within ten (10) days after initiation of contract. To avoid unnecessary delays, new contractor

**PERSONNEL
SCREENING,**
Continued

personnel may begin work while the OPM screening is in progress, **provided contractor personnel have already completed pre-screening requirements by their employer.**

Vendors must verify that the following minimum pre-screening requirements have been done for their EPA contractor personnel:

- C Check of prior employment record.
- C Check of references.
- C Verification of claimed degrees/education/military service.
- C Verification of signed statement that the employee has never been convicted of a felony.

Additional useful EPA personnel screening information can be found in the Office of Inspector General's EPA Personnel Security Manual.

10.2
INFORMATION
SYSTEM ACCESS
ADMINISTRATION

The level and type of application and system access provided to Agency and contractor personnel must be periodically reviewed. The objective of this review is to ensure the following conditions are enforced:

- C The information system limits access to authorized personnel.
- C Access lists are up-to-date (i.e., access rights are removed for terminated and transferred employees and contractors).
- C The level of access provided to each individual is limited to the level required to complete his/her job responsibilities.

Responsibilities for information system access administration include the following:

- 1) The individual assigned responsibility for a general support system or major application must designate the individual(s) responsible for maintaining application/system access control lists. If the application/system's information sensitivity is moderate or high, this functional position must be staffed by EPA personnel or by contractor personnel with the appropriate level of screening.
- 2) Information managers responsible for general support systems and major applications must ensure that access controls are reviewed monthly. During the review, verify that the access list has been updated for terminated and transferred individuals. Test the information system's access control mechanism to ensure that it cannot be bypassed. Ensure that each individual assigned access has only the

INFORMATION
SYSTEM ACCESS

ADMINISTRATION,
Continued

level of access defined by his/her manager. Periodically review the application/system audit trail to verify that individuals are not exceeding or trying to exceed their access rights.

- 3) Managers must provide **immediate** notification to the designated general support system and major application personnel when EPA employees or contractor personnel are transferred or terminated.
 - 4) Managers must document the applications and systems for which new or transferred individuals require access. In addition, the documentation must define the level of access required for each system and/or application, e.g., read, write, update, design, etc. This documentation must be provided to the designated application/system personnel for use in assigning access rights.
-

10.3
SEPARATION OF
DUTIES

Separation of duties means dividing roles for sensitive positions, such as cutting checks, among multiple personnel to ensure that no one person has sole control over a sensitive process.

Separation of duties is an important security concept when dealing with the types of processing required for financial and payroll applications. The concept also applies to processes within general support systems, such as providing and verifying information system access rights, reviewing audit trails, and establishing and testing security controls. Consider the fraud cases that are covered by the news media, including setting aside money from one account to another, browsing data files for information that can be sold, etc. It is more difficult for an individual to conceal errors and irregularities if he or she does not control all aspects of an activity. Therefore, sensitive functions must be separated so that no single individual controls the entire process. An example of this concept is separating the functions of cash handling and bookkeeping. The bookkeeper no longer handles the cash, and the cash register clerk cannot adjust the books to hide cash shortages.

SEPARATION OF
DUTIES, *Continued*

To the extent possible, the following functions within the Agency should be assigned to different individuals:

- C Data Creation and Control Functions
-

- Data collection and preparation
- Data entry
- Data base administration

- C Software Development and Maintenance Functions
 - Applications programming
 - Design review
 - Application testing and evaluation
 - Application maintenance

- C Security Functions
 - Security implementation
 - Review of security controls
 - Security audits and audit trail review

In some cases, such as where work is performed on individually assigned PCs or workstations, it is difficult to separate these functions. The need for separation of duties must be based on the sensitivity of the information and the risk of loss or harm. Separation of duties is mandatory for all financial applications (relating to check issuance, funds transfer, and the like) where misuse could cause a direct financial loss. For example, the task of preparing payment vouchers must be kept separate from the task of approving payments. This requirement also applies to PC-based financial applications. The above list of functions is not necessarily comprehensive for all situations.

**10.4
TERMINATION/
SEPARATION**

Supervisors and contract administration personnel (DOPO, WAM, etc.) must ensure that the following activities are performed for all personnel, including contractors, leaving, changing jobs, or extended absences:

- C Change or cancel all passwords, codes, user IDs, and locks. Disable user ID for extended absences (60 days).

- C Update access control lists, mailing lists, etc.

- C Collect all keys, badges, and similar items.

- C Reconcile any financial accounts over which the employee had control.

- C Ensure electronic records are assessable and properly secured, or

**TERMINATION/
SEPARATION,
*Continued***

appropriately disposed of.

In the event an individual must be removed or laid off, the above actions must be completed *immediately*. In addition, the employee, or contractor, should be rotated to a non-sensitive position before the employee is notified that he or she will be terminated. While this may seem extreme, angry and demoralized employees have been known to sabotage programs, erase data bases, and plant computer viruses.

The DD, or the DD's designate, must ensure that these procedures have been accomplished for Agency personnel. Contract administration personnel must ensure these activities are specified and implemented through contractual mechanisms for contractor personnel.

10.5 TRAINING

EPA organizational information security programs must provide security training to sustain the implementation of security procedures presented in the *ISM*. EPA's information security training program includes both information security awareness training and specialized training. The information security program is responsible for providing security awareness training criteria. Each program and region must establish a training program based on these training criteria.

Information security awareness and training is required for every user and must be tailored as required by 5 CFR 930.301 to meet the functional responsibilities of the user. Training requirements and responsibilities should be identified in acquisition documents.

Information security awareness training emphasizes the vulnerabilities of and risks to EPA information systems and informs individuals of their responsibilities for maintaining information availability, integrity, and confidentiality. Information security awareness training is designed to provide an understanding of the following concepts:

- C Threats to and vulnerabilities of computer information systems.
- C Agency policy and goals for protecting EPA's information.
- C Good security practices to protect facilities, equipment, and information.
- C Information security roles and responsibilities.
- C Basic concepts of risk management, contingency planning, and

TRAINING,
Continued

security throughout the information system's life cycle.

**Three Security
Training Phases**

Information security awareness and training must be provided to EPA employees in the following 3 phases:

1. Initial awareness training is provided to new employees within 60 days of employment.
2. Continuing training is provided whenever there is a significant change in EPA's information security environment or when an employee enters a new position.
3. Refresher training is provided annually.

EPA program offices and regions shall provide periodic specialized information security training as appropriate to employees with specific information security responsibilities, such as information managers, ISOs, and SIRMOS. Specialized information security training informs these employees of how to carry out their information security responsibilities.

The Information Security Awareness Training Addendum to EPA's InfoSec Program Plan details the Agency's information security awareness training program and provides criteria for this training that are tailored to meet employees' and other users' functional responsibilities.

[This page intentionally blank.]

11.0 TECHNICAL SECURITY

Technical security controls are an important component of an effective security program. However, technical controls, in and of themselves, will not ensure that information is adequately protected. To be effective, technical security controls must support security policy and be selected based their ability to maintain an acceptable level of risk for Agency information systems and applications. The type of technical controls used must balance risk against the needs of information users. Use too many controls and an information system becomes almost unusable. Too few, poorly implemented, or untested controls lead to a false sense of security.

To be effective, technical security controls must support security policy. In addition, controls must be selected following a risk management approach that balances the level of risk against the needs of information users. Use too many controls and a information system becomes almost unusable. Too few, or poorly implemented, controls will provide a false sense of security. This Section describes how technical controls support security policy, what types of controls are required, and how controls must be implemented, tested, and documented.

This Section discusses the following topics:

- C Support for Agency and organizational security policy.
- C Required technical controls.
- C Testing and documenting controls.

The following subsections discuss technical controls within general categories. The Information Security Manual cannot specify the technology used to implement these controls. Control selection must be based on level of risk and the cost-effectiveness of a given control in managing that risk.

11.1 SUPPORTING AGENCY AND ORGANIZATIONAL SECURITY POLICY

General support systems and major applications must include the controls necessary to ensure that information is adequately protected. Technical controls must be chosen based on their ability to support and implement Agency and organizational security policy. For example, organization policy stipulates that all system users be authenticated. The associated technical control is password protection. However, the effectiveness of technical controls is limited by the ways in which the control is installed and managed. Password protection will only be effective if both a strong technology is employed and it is appropriately managed and periodically tested to ensure that it is used correctly.

**11.2
REQUIRED
TECHNICAL
CONTROLS**

Technical controls must be chosen based on the security principles discussed in Section 3, including cost-effectiveness and the control's ability to provide an adequate level of security, enforce least privilege, and limit use to authorized personnel only.

EPA information resources must be protected through the use of the following types of security controls. The technology used and the cost to acquire and implement these types of technical controls will vary depending on the acceptable level of risk determined for the information, general support system, or major application.

- C Access Controls
- C Backups
- C Configuration Management
- C Physical and Environmental Controls
- C Network Access
- C Communications
- C Audit Trails

The following subsections describe each of these categories of controls. Additional technical controls may be required depending on the specific environment, threat and the information's sensitivity. Consult sections 4.0 - Information Sensitivity and Security Goals, 5.0 - Threats, 7.0 - Internet Use, 8.0 - Public Access, 9.0 - Flexiplace for additional requirements, as appropriate.

L Note:

This Section does not describe controls based on their ability to preserve information availability, integrity, or confidentiality. Many controls provide protection for multiple goals simultaneously. Where a technical control applies primarily to one specific security goal, it is noted in the discussion.

11.2.1

Information system access controls are used to accomplish the following

**ACCESS
CONTROLS**

objectives:

- C Limit access to authorized personnel.
- C Limit the level of access provided to each individual to the level required to complete his/her job responsibilities.

When more than one person uses a single computer information system, physical, procedural, and/or technical measures must be provided that allow the identification and authentication of individual users and prevent access by unauthorized persons.

For information systems containing information of moderate sensitivity, implement physical, procedural, and technical measures that restrict the functional capabilities of individual users. Individual users should still have the capability to manage access (e.g., create, read, modify, or delete) by other users to his or her information and applications.

For highly sensitive information systems, install logical alarms to alert security personnel if intrusion occurs and restrict and log individual user access by system resource, application, and file. Authorization to access system resources, applications, and files must be confirmed by the information managers/owners and must be reconfirmed periodically (at least every six months).

Use automatic workstation log-off, time-out, or equivalent features for information systems where the information sensitivity is medium or high.

Use discretionary access controls to grant access in database management systems where information sensitivity is medium. Use mandatory access controls to grant access in database management systems where information sensitivity is high. Log events to data tables containing information of high confidentiality or high integrity.

Access to and use of medium or highly sensitive information in database management systems must be well defined, controlled, and communicated to all users.

11.2.2

BACKUPS

Back up computer systems and applications on a regular basis. Backups must include the following: data and files, end-user applications, source program files, loadable versions of all software, and compilers. Backups of commercial application software must be maintained in accordance with software licensing agreements. A backup of operating system software must be maintained and updated as new releases are received. Maintain at least one generation of backups.

Back up computer systems and applications on a basis commensurate with the risk of loss or harm that would result if the data were lost or unavailable. For information systems containing information of moderate or high sensitivity, maintain at least two generations of backups.

Managers of applications or systems must take a new copy of the backup to an offsite location at least once per month. Managers of applications or systems containing information of moderate or high integrity or availability must take a new copy of the backup to a secured offsite location at least weekly. Backup rules must take into consideration the needs of all the users of the system.

L Note:

NOTE: If the information system contains confidential information, then backups are confidential as well. Protect backups according to EPA requirements for confidential data.

11.2.3 CONFIGURATION MANAGEMENT

Catalog all files, and maintain licenses for all software. Register all licensed software with the author or vendor before it is used. Software must be tested on an equivalently configured system and determined to be safe (free of malicious design/code) for use in its intended environment.

Managers of moderately and highly sensitive information systems must develop and maintain a configuration management process to monitor changes to any security-related and other software, hardware, or procedures for the information system.

Information systems containing highly sensitive information must have the provision for the appropriate data bases to be stored off-line.

**11.2.4
PHYSICAL AND
ENVIRONMENTAL
CONTROLS**

Physical security is required to protect information systems against unauthorized access, theft, or destruction. Take proper measures to minimize the effects of dust, water, temperature, humidity, and ventilation on information systems. Install power surge protection for all hardware. Install alarms for information systems containing highly sensitive information to alert security personnel when intrusion occurs and to warn of failure in environmental controls.

Systems for which availability is a significant concern must use a backup power supply, where cost-effective. All systems must have an uninterruptable power supply (UPS) to provide for an orderly shut-down and protect against operating system and file loss or corruption.

**11.2.5
NETWORK
ACCESS**

Require passwords for access to or from any network. Passwords must have a minimum of six characters. Passwords must include a mix of alpha and numeric characters. Use software that provides error checking and some error correction capability when performing file transfers using networks. Obtain written consent identifying other network nodes authorized to access the system node, prior to enabling any network connection or interconnection.

**11.2.6
COMMUNICATIONS**

Communications links connecting a computer system to other systems, networks, workstations, or terminals must be approved by management before the connection is implemented.

Document communication paths for the information system and establish a well-defined path for initial user identification and authentication processes. Permit only controlled dial-up access and authorized connections to networks. Dial-up access must be controlled by limiting access to only authorized users of EPA information through the use of passwords and user IDs. Authorized connections are those connections for which the LAN manager has made explicit approval for connection to the LAN. Information managers must evaluate threats and risks associated with connections to wide-area and/or internationally linked networks. Use additional measures such as dial-back protection, one-time password technology, etc. to enhance the identification and authentication controls associated with dial-up connections to the EPA network unless another approach is approved in writing by the CIO. EPA network security policy

COMMUNICATIONS
Continued

defines minimum technical controls when connecting to the Internet.

Encryption technology or other acceptable means must be used for the transmission of confidential information. Cryptographic technologies should be applied to information where integrity is high or possibly medium sensitivity.

11.2.7
AUDIT TRAILS

Major applications containing moderately and highly sensitive information and all general support systems must generate audit trails of accesses and changes to the system and to information and applications at the individual user level. An audit trail documents activities and/or events associated with files or system usage by recording the date, time, and responsible person/device. Access to trails must be restricted to a well-defined group of users authorized by the responsible information manager. It should be noted that audit trails are used to ensure that individuals are held accountable for their actions. The need for accountability must be fully evaluated for public access information systems, because it may not be possible to ensure that all public users are individually identifiable. Review audit logs on a daily basis for major applications containing moderate to highly sensitive information and all general support systems to identify security incidents. Use audit log reduction, filters, exception alerts, or similar techniques to reduce workload and log volumes, for the purposes of this review.

11.3
TESTING AND
DOCUMENTING
CONTROLS

The information security planning process provides the framework for testing and documenting controls. Controls must be evaluated for effectiveness as security plans are completed and prior to authorization of the system or application, and periodically retested, as implemented, during the security control review process (conducted at least every three years).

In addition to performing the review or audit of security controls required by OMB A-130, perform the following control reviews annually for all general support systems and major applications containing highly sensitive information. These reviews must address access controls and integrity controls. The access controls shall be reviewed to ensure the access, as implemented, is based on the concepts of least privilege and proper separation of duties. The system integrity controls shall be reviewed to ensure that the system libraries and configuration settings are maintained in accordance with EPA requirements and vendor guidelines. Also ensure that unnecessary and/or outdated versions of system files, including utilities,

TESTING AND

**DOCUMENTING
CONTROLS,**
Continued

have been properly removed as part of the integrity controls reviews. Software tools are recommended to support these reviews, save time and allow more frequent reviews for highly sensitive information systems.

[This page intentionally blank.]

12.0 ORGANIZATIONAL SECURITY PROGRAMS

EPA's Information Security Program is centrally managed through OEI. The Program defines EPA requirements for information security. However, each EPA organization, i.e., offices, regions, divisions, branches, etc., uses various categories and sensitivity levels of information across multiple computing platforms to meet their mission requirements. Consequently, each Primary Organization Head must establish an information security program, based on EPA's central Information Security Program, that is tailored to the specific types of information, information systems, and computing platforms throughout the organization and to the manner in which the information is used.

Each organization within EPA (i.e., Programs and Regions) must establish a security program that addresses the security requirements specific to their organization. This Section describes the minimum requirements for a security program based on EPA and Federal mandates.

This section discusses the role of EPA's central Information Security Program and presents requirements for the following organizational security program areas:

- C Organizational Information Security Program Goals.
- C Mandated Information Security Program Requirements.
- C Organization-Specific Security Procedures.

The following subsections provide information for each organization to use in implementing a security program. While organizations must tailor their security programs according to the types of information and information systems they use, each program must still meet EPA's basic information security program requirements.

12.1 ROLE OF EPA'S CENTRAL SECURITY PROGRAM

EPA, like many other Federal agencies, is organized decentrally. Agency policy and procedures are defined centrally and must be implemented and administered at the program office and regional levels. EPA's central security program defines the strategic direction for the Agency's security program, establishes basic structural requirements for organizational programs, and defines overall security roles and responsibilities. This Information Security Manual is issued through the central program and presents information security policy and procedure derived from the EPA *IRM Policy Manual*, Chapter 8, *Information Security*. Each organization must establish an organizational information security program that implements these Agency-level information security policy and procedures.

**12.2
ORGANIZATIONAL
INFORMATION
SECURITY
PROGRAM GOALS**

Each organizational security program must achieve the following goals.

- C Information is protected commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access or modification. Systems and applications must operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
- C Access to information, support systems, and applications is provided to authorized personnel only.
- C Federal and Agency-level information security policies and procedures are implemented.
- C Roles and responsibilities for information security throughout the organization are explicitly defined.
- C The resources required for implementing the program are identified and assigned to the program.

The procedural and technical methods used to achieve these goals will differ from organization to organization because security controls must be based on the types of information and information system platforms, threats, vulnerabilities, and level of risk for a given organization. To be effective, all security controls must support the Program's policies and goals. Section 11 of this Manual discusses technical security controls.

**12.3
MANDATED
INFORMATION
SECURITY
PROGRAM
REQUIREMENTS**

Appendix III of OMB Circular A-130, *Security of Federal Automated Information Resources*, stipulates the minimum security controls to be included in agency programs for their general support systems and major applications. The following four controls are mandated:

- C Assignment of Responsibility
- C Security Plans
- C Periodic Review of Security Controls
- C Authorization for Processing

MANDATED

The following subsections present EPA's requirements for each of these

**INFORMATION
SECURITY
PROGRAM
REQUIREMENTS,**
Continued

information security program areas. These requirements are also discussed in EPA's *Information Security Planning Guidance*.

**Assignment of
Responsibility**

The Division Director must designate an individual to be responsible for the security of each general support system and major application within the division. Assignment of responsibility must be *in writing* and retained as an official document. If responsibility is not formally assigned, a deficiency should be identified pursuant to OMB Circular A-123, *Management Accountability and Control*, during the periodic security control review process.

Individuals must have a specific skill set in order to be assigned responsibility for security. For a general support system, the individual must be knowledgeable in the technology used by the system and in providing security for that type of technology. For a major application, the individual must have an understanding of the types of information and processes supported by the application and the controls used in securing the application.

Security Plans

Organizational security programs must define specific procedures and responsibilities for completing security plans for the general support systems and major applications within their purview. Note that all general support systems and major applications must have a security plan.

Specific issues to be considered within the security planning process include:

- C Systems or applications owned or operated by multiple organizations.
- C Definition of criteria for consolidating small general support systems into a single plan.
- C Roles and responsibilities for the security plan review process.

Security Plans,
Continued

Pertinent sections of the security plans, e.g., rules of behavior, must be provided to information system users. *Certain sections of the security plan,*

and the security plan when handled as a whole document, should be considered sensitive, because details are provided on system or application vulnerabilities. Care must be taken to securely distribute and control the entire security plan, or those portions which identify vulnerabilities, when it is disseminated. All organizational security planning procedures must comply with the planning requirements presented in Section 13 of this manual.

**Periodic Review
of Security
Controls**

Computer technology, information system users, information system data, risks, and security requirements are constantly changing. Information security may be affected by new technology, system connections, and threats. New or enhanced technology often results in additional vulnerabilities. In addition, users are becoming more technically self-sufficient. Due to these factors, many security procedures and technical controls become outdated and information and information system security must be periodically reassessed.

Each organizational security program must define procedures and responsibilities for conducting periodic security control reviews for their general support systems and major applications. The following paragraphs present the requirements for periodic security control reviews:

General Support Systems
<p>The security control review must consist of an independent audit or self review. The organization must define when self reviews are sufficient and when independent audits are required. The type of security control review must be commensurate with the system's level of risk.</p> <p>Security reviews must be conducted when major modifications occur, but at least once every three years. Major modifications include, but are not limited to the following:</p> <ul style="list-style-type: none">- Changes in the telecommunications environment, e.g., addition of new equipment such as routers.- Addition of external connections.- Modification or enhancement of system software.

**Periodic Review
of Security
Controls,**

Major Applications

Continued

The security control review must consist of an independent review or audit of the major application at least every three years.

Because the security of a major application is affected by the risks and vulnerabilities of the support system(s) in which it operates, the scope of the security review must include the general support system in which the major application operates. The results of the general support system's security control review and security plan can be used to provide the needed information.

The time interval for periodic reviews must be commensurate with the value of the information processed. The interval period must be at least every three years.

For both general support systems and major applications, a deficiency should be identified pursuant to OMB Circular A-123, *Management Accountability and Control*, if the following components are not in place:

- C Formal (i.e., written) assignment of responsibility.
- C Security plan.
- C Written authorization to process.

Independent reviews or audits should be independent of the manager responsible for the application or system, as appropriate.

Authorization to Process

A management official must authorize in writing the use of each general support system and major application. This official cannot be the person assigned responsibility for the security of the general support system or major application.

Authorization must be based on the security plan because the plan defines the security controls for the general support system or major application. The manager must determine if the plan, as implemented, provides adequate security. Management's signature means that they are accepting the risk associated with processing—they agree that the general support system or major application is at an acceptable level of risk.

Authorization to Process,

Authorization to process must be obtained *prior* to operation or upon significant modification. General support systems and major applications

Continued

must be re-authorized at least every three years.

**12.4
ORGANIZATION-
SPECIFIC
SECURITY
POLICIES AND
PROCEDURES**

While EPA's central security program defines the overall policy, each organization must develop organization-specific policies and procedures for implementing their program. Organizations must develop procedures that implement the following requirements for their security program:

- C Conducting and tracking training for general support systems and major applications.
- C Developing and conducting awareness training.
- C Explicitly assigning security roles and responsibilities.
- C Completing continuity of support and contingency plans.
- C Defining an acceptable security baseline.
- C Accomplishing minimum security program requirements, i.e., assignment of responsibility, security plans, periodic security control reviews, and authorization for processing.
- C Enforcing security policy.

In addition, organizations may define policies and procedures for specific areas of concern or security issues within the organization. Internet access and flexiplace are examples of areas in which management may develop issue-specific policies. While this type of policy is intentionally specific to an individual organization, the policy must align with Agency policy. For example, the Agency restricts Internet access to authorized use only. An organization cannot develop their own less-restrictive policy.

For an information security program to be effective, management must

12.5
SECURITY
PROGRAM
IMPLEMENTATION

ensure that information is readily and constantly disseminated regarding security program objectives and responsibilities.

Management must formally document security program requirements and regularly evaluate its program to ensure that the program is meeting its goals. Security violations must be monitored and evaluated. Where necessary, new or revised policies may need to be issued to ensure that organizational information assets are adequately secured.

[This page intentionally blank.]

13.0 SECURITY PLANS

Automated information systems face a wide range of threats that can compromise information availability, integrity, and confidentiality. Acts of nature such as lightning, tornados, and floods may damage hardware or halt application processing. Saboteurs can destroy data and hardware, plant viruses or malicious code, and disclose confidential information. Accidents and errors can compromise Agency information. All general support systems and major applications must have a security plan in place to ensure that the risks posed by these, and other, threats can be appropriately managed.

All EPA general support systems and major applications must have a current security plan in place that has been properly reviewed and approved. This Section discusses security planning requirements and plan content, review, and approval.

The security planning process provides the opportunity to identify threats, assess risks, and establish the necessary safeguards. The following subsections discuss the need for security at the information system level, the role security plans play in securing information systems, and the security planning process within EPA.

13.1 POTENTIAL IMPACT ON AGENCY'S MISSION

EPA policy is to ensure that all information resources within EPA are adequately protected. In developing a security plan, the security requirements of the Agency's major applications, general support systems, and associated information are identified, evaluated, and documented. If security requirements are not met, information resources may be compromised and the Agency may not be able to fulfil its mission requirements. Consider the following events:

- C *Access to computing services or critical information is not available when needed.* What will happen if Agency programs do not have access to the necessary information or automated services to complete time critical functions such as congressional reporting, budget planning, financial and payroll services, enforcement actions, and environmental monitoring data collection?
- C *Data is intentionally or unintentionally altered.* Consider the affect of accidentally providing inaccurate or altered data to the public, congress, or such administrative functions as financial management and payroll.
- C *Confidential data is intentionally or accidentally disclosed.* What will happen if unauthorized personnel (inside or outside EPA) have access to enforcement, legal, CBI, budget, or such personnel information as social security numbers, home addresses, etc.?

**POTENTIAL
IMPACT ON
AGENCY'S
MISSION, *Continued***

EPA's stakeholders and partners and the regulated community assume that the Agency adequately protects the information they provide from unauthorized alteration and, where necessary, from unauthorized disclosure. If EPA cannot protect externally provided data appropriately, the Agency may lose the confidence of its stakeholders and partners and, therefore, their future cooperation.

**13.2
HOW DO
SECURITY PLANS
PROTECT EPA'S
INFORMATION?**

How do security plans help ensure that information resources are adequately protected? Security plans provide the vehicle for identifying an information systems' security and privacy requirements and defining how these requirements are met. The security planning process provides a structured approach for identifying the following:

- C Information sensitivity and information system security requirements.
- C Threats and vulnerabilities.
- C Current level of risk.
- C Acceptable level of risk.
- C Controls and effectiveness of the controls currently used to protect the information system from threats and vulnerabilities.
- C Need for additional controls with planned schedules and responsibilities identified for implementing these controls.
- C System- and application-level policies and rules of behavior.

In addition to ensuring that information security requirements are identified and met, security plans provide several other benefits:

- C Plans provide management with detailed information regarding the systems and applications for which they are ultimately accountable. The plan contains information for management to use in determining that a system or application is at an acceptable level of risk.
- C Plans detail the methods used to protect the system or application and its associated information. Information owners have a means of determining that their information is adequately protected.

Security plans become local policy for EPA Headquarters and regional major applications and general support systems.

13.3 SECURITY PLANNING MANDATES

Federal and EPA mandates require security plans for all Agency general support systems and major applications.

First and foremost, plans are required by law, specifically the Computer Security Act. In addition, plans for general support systems and major applications are required by Federal and Agency policy. OMB Circular A-130 requires plans for all general support systems under the presumption that all general support systems contain some sensitive information which requires protection to assure its integrity, availability, or confidentiality. All Federal applications require some level of protection. Major applications are those requiring special management oversight or attention to security, and therefore, must have a security plan. Security for other applications must be addressed in the security plans for the support systems in which they operate.

13.4 EPA'S SECURITY PLANNING REQUIREMENTS

EPA's *Information Security Planning Guidance* provides directions for completing and prescribes the format required for Agency general support system and major application security plans. Information managers are responsible for ensuring that security plans are completed, adhere to the required format, include the appropriate level of detail, and are approved by management.

Security plans must include the following information:

- C Information system description and background information.
- C Type(s) of information processed.
- C Applicable laws, regulations, and standards.
- C Status of risk management activities.
- C General support system and major application security plan components, listed in the following table.

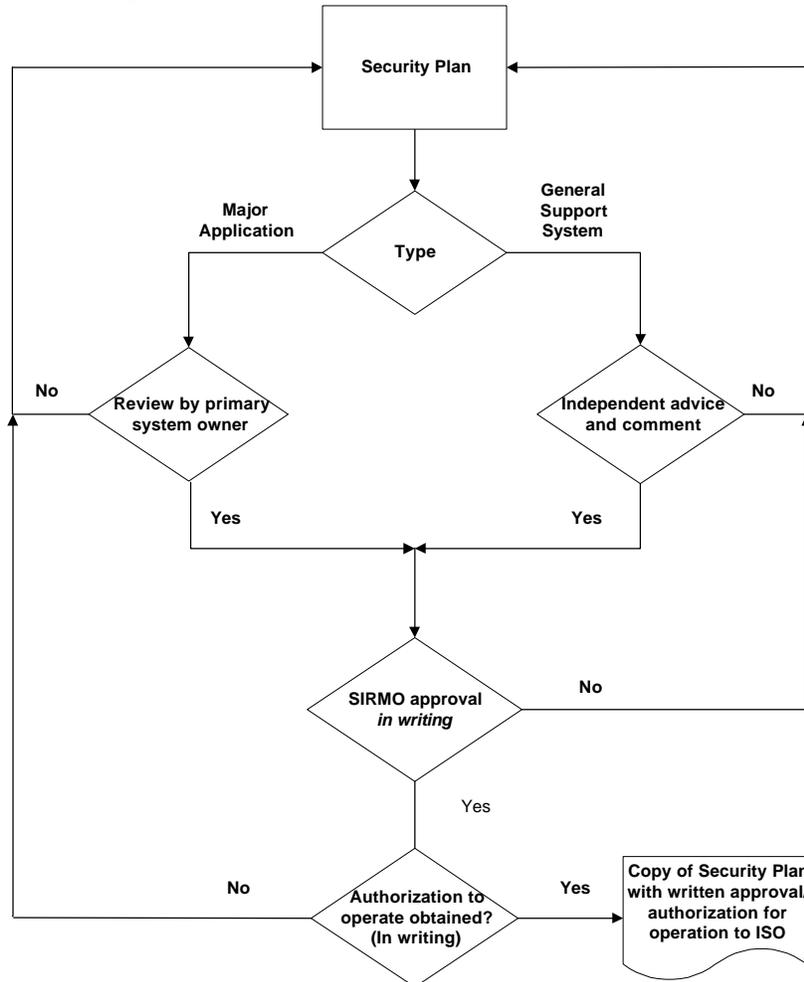
General Support Systems	Major Applications
System Rules	Application Rules
Training	Specialized Training
Personnel Controls	Personnel Security

EPA'S SECURITY PLANNING REQUIREMENTS,
Continued

General Support Systems	Major Applications
Incident Response Capability	Contingency Planning
Continuity of Support	
Technical Security	Technical Controls
System Interconnection	Information Sharing
	Public Access

Each of the above components is described in detail in the Information Security Planning Guidance document.

EPA Security Planning Process



**EPA'S SECURITY
PLANNING
REQUIREMENTS,**
Continued

As illustrated in the figure on the preceding page, security plans are but one component of EPA's security planning process. Plans must be completed based on an assessment of the system's or application's risk environment and current security measures as implemented, additional controls must be defined and implemented as necessary, and the plan must be reviewed and approved by the appropriate SIRMO. Systems and applications must receive management authorization to process prior to operation, and be re-authorized at least every three years or upon significant system change.

**Sharing Security
Plan Information**

Security plans serve as the local policy for EPA general support systems and major applications. Therefore, portions of the plan must be shared among system and application owners, users, and managers of other support systems and applications that may be impacted by the security of the information system. However, as previously stated, ***security plans contain information that must be protected from unauthorized disclosure. Security plans present security vulnerabilities that, in the wrong hands, could be used to gain unauthorized access to the information system and information.*** Therefore, care must be exercised in determining which portions of the plan can be shared.

Portions of security plans meant for distribution among information system users include:

- ⊆ Rules of behavior and consequences of non-compliance.
- ⊆ Remote access and flexiplace rules (if applicable).

The following portions of security plans are sensitive and are to be distributed to authorized personnel only.

- ⊆ Risk analysis/risk assessment.
- ⊆ System or application vulnerabilities and planned controls.
- ⊆ Lists of information system controls.
- ⊆ Contingency plans, or continuity of support plans.
- ⊆ Public access controls (if applicable).

Keep in mind that major application security plans should be reviewed by and must be provided to the manager of the general support system(s) on which the application operates. Furthermore, general support system managers must provide a copy of their security plan to the managers of the major applications operating on their system.

[This page intentionally blank.]

14.0 MANUAL INFORMATION SECURITY

This section describes the protective measures that should be taken to ensure adequate protection of collections of paper and microform (microfiche and microfilm) records. The focus here is on an organized collection of records that are relied upon as a manual information system.

This Section discusses responsibilities, threats, and security procedures for information maintained in a non-automated environment.

14.1 RESPONSIBILITIES FOR MANUAL INFORMATION

The following two situations apply:

- C Information managers develop the security requirements for the information, based on the procedures presented here, and are responsible for ensuring that the necessary information security controls are in place.
- C Records Management Officers assign responsibility for the physical custody of the records and make sure that custodians implement these procedures properly.

For specific guidance on protecting manual records containing CBI and other types of confidential information, see the *EPA Records Management Manual*. For guidance concerning written requests for documents under the *Freedom of Information Act (FOIA)*, refer to the *FOIA Manual* or contact the FOIA Office.

14.2 RELATIONSHIP TO OTHER PROCEDURES

Over the years, EPA has developed several sets of procedures governing specific categories of sensitive information. The great majority of these existing procedures deal with some type of confidential information, especially confidential business information. These procedures are typically issued by EPA organizations with statutory authority for the information (e.g., the Office of Prevention, Pesticides, and Toxic Substances for *Toxic Substances Control Act (TSCA)* or *Federal Insecticide, Fungicide and Rodenticide Act (FIFRA)* confidential business information). EPA employees must adhere to all of these organizational standards and procedures, as well as to the procedures presented here.

RELATIONSHIP TO

The scope and nature of these other types of information procedures include

**OTHER
PROCEDURES,**
Continued

the following:

- C The EPA *Records Management Manual* defines the policies and procedures for records management activities including the following:
- Procedures for the disposal and retirement of Agency records to a Federal Records Center according to EPA Records Control Schedules and for the retrieval of Agency records from a Federal Records Center;
 - Policies and procedures pertaining to vital Agency records;
 - Policies and procedures regarding manual filing equipment, supplies, and file maintenance; and
 - Procedures for the documentation and preservation of electronic records.

The objectives of the EPA Records Management Program include preserving records of value and disposing of or transferring records no longer current. In addition, this Program is concerned with the preservation of vital Agency information: information that is vital to the essential functions of the Agency or that is essential to the legal rights and interests of individual citizens and the Government. The Program also provides policies and procedures to establish programs to maintain and protect Agency records as specified in 41 CFR 101.

- C The Office of Administration and Resources Management (OARM) has issued procedures governing NSI in the *National Security Information Handbook* and *Privacy Act* data. The NSI handbook also contains self-inspection procedures for organizations handling NSI.
- C The Office of Prevention, Pesticides, and Toxic Substances has developed manuals governing both *TSCA* and *FIFRA* confidential business information.
- C The Office of Solid Waste and Emergency Response (OSWER) has issued procedures concerning *Resource Conservation and Recovery Act (RCRA)* confidential business information.

RELATIONSHIP TO

- C The Office of Enforcement and Compliance Assurance (OECA) has established enforcement docket security procedures for handling and

**OTHER
PROCEDURES,**
Continued

- disposing of docket reports.
- C Within the Office of Air and Radiation (OAR), the Office of Mobile Sources (OMS) has established procedures for handling proprietary data received from automobile manufacturers and the Office of Air Quality Planning and Standards (Emission Standards and Engineering Division) has procedures for safeguarding the confidential business information it receives.
 - C The Office of Inspector General (OIG) has procedures dealing with confidential information obtained during the course of investigations and audits.
 - C The Office of Water (OW) has developed procedures related to trade secret data obtained under Section 308 of the *Clean Water Act*.

Most of these procedures contain special instructions and handling requirements. To make sure they are in compliance, EPA employees must review these procedures when appropriate.

**14.3
THREATS TO
MANUAL
INFORMATION**

Information in hard copy or microform is subject to threats that can affect information availability, integrity, and confidentiality.

Threats to availability include the following:

- C **Theft or Loss.** Paper and microform records are small, light, and easily moved. A record can be stolen or can be accidentally or intentionally misfiled.
- C **Accidental destruction of records.** A record may be accidentally destroyed or lost through an act of nature (such as a flood or fire) or through human error (such as inadvertently throwing it away).
- C **Deliberate destruction of records.** Records can be deliberately destroyed. Such destruction can be the result of random vandalism, but it can also be the act of an employee who has been dismissed, disciplined, or is hostile to the mission of the office.

**THREATS TO
MANUAL**

The integrity of manual information can be compromised by the following threats:

INFORMATION,
Continued

- C Deliberate distortion of records through fraud and sabotage.** The integrity of records can be damaged by the deliberate actions of individuals with access to the records. These actions could be motivated by revenge (for example, by recently reprimanded employees) or could be intended to perpetrate or cover up fraud, mismanagement, or waste.
- C Accidental damage.** This occurs when individuals inadvertently and unknowingly change records. While this is a common threat to automated information systems, it is less prevalent for manual systems. It would occur, for example, if records became disorganized. If the disorganization went undetected, decisions could be made based on information that seemed complete, but was not because crucial information had been misfiled elsewhere.

Threats to confidentiality are largely problems of access control. Specific threats to the confidentiality of manual information include the following:

- C Unauthorized disclosure.** If rooms or cabinets housing confidential records are not secure, unauthorized individuals can open them and review the records. Unauthorized disclosure can also occur if authorized individuals deliberately share confidential records with unauthorized individuals. Individuals are responsible for safeguarding confidential information that has been retrieved (printed or displayed) from an automated source.
- C Typewriter and printer ribbons.** Confidential information can be deciphered from typewriter and printer ribbons that have been used to produce confidential reports.

14.4
PROCEDURES TO
PROTECT
MANUAL
INFORMATION

PROCEDURES TO
PROTECT
MANUAL

The controls presented in the following table are required to protect the availability, integrity, and confidentiality of records within manual information systems. However, the information manager may perform an assessment of the impact should the availability, integrity, or confidentiality of the records be compromised. The EPA's *Risk Analysis Guideline* and FIPS PUB 65, *Guideline for Automatic Data Processing Risk Analysis*, contain the criteria and procedures for performing this assessment. If the result of this assessment is that the cost of the controls outweigh the potential impacts, the information manager may implement more cost-effective controls.

INFORMATION,
Continued

Procedures to Maintain Availability. To maintain the availability of physical documents, procedures and controls must be implemented to ensure that the physical records are not damaged, lost, or removed without authorization. These controls include environmental and access controls, fire protection, document tracking, and backups.

Procedures to Maintain Integrity. The protective techniques needed to ensure integrity represent a combination of those associated with maintaining availability and those associated with preserving confidentiality. As is true of information maintained in an automated system, copies of manual records produced to enhance availability can aggravate the problem of preventing the inappropriate disclosure of information. Integrity involves elements of availability because, if information is altered or partially destroyed, an intact backup copy is essential. On the other hand, integrity involves elements of confidentiality because preventing fraud and sabotage are largely problems of controlling access.

Procedures to Preserve Confidentiality. Preserving confidentiality involves controlling access to information and records. Access controls for manual information systems are of two types: physical, such as door locks, and administrative, such as lists that specify who is allowed access to the records.

The following tables list manual security controls and the security goals for which they provide protection.

Manual Security Controls

Manual Security Controls	A	I	C
<p>Environmental Controls. To avoid water damage, records should not be stored directly beneath sprinkler heads or water pipes. They should not be located near boiler rooms or water heaters. To prevent water damage to paper records, these materials should be stored in enclosed filing cabinets. Experience has shown that this greatly reduces damage even if there is a water problem.</p>	T	T	
<p>Access Controls. The information owner must establish, for the information custodian, a list of individuals who are allowed access to the records. The information manager should review the list and update it quarterly.</p>	T	T	T

Manual Security Controls, Continued

Manual Security Controls	A	I	C
<p>Information owners must also protect records that are requested under the Freedom of Information Act and reviewed on EPA premises.</p> <p>Recommended controls to protect the future availability of these records include:</p> <ul style="list-style-type: none"> C Maintain constant supervision of the records and the records-handling of the viewers; C Allow only one box/folder to be open at any one time during the viewing process; C Require that all carried parcels, briefcases, purses, etc., be stored away from the viewing area; and C Ensure that no official EPA records are removed from EPA premises. 	T	T	
<p>Document Control and Tracking. To prevent the loss of records, a document control and tracking system should be established. This tracking system may be automated or manual. In either case, the system should include:</p> <ul style="list-style-type: none"> C Control Number. A unique identifier, such as a document control number, for each document in the collection of records. C Tracking. A cradle-to-grave tracking capability, which follows a record from the time it is received or written until it is destroyed or transferred elsewhere. 	T	T	
<p>Whenever possible, records should be stored in a fireproof file cabinet.</p>		T	
<p>Accessible Backup Copies. Storage locations that require one to two days notice to retrieve records are of limited usefulness. Therefore, for critical collections, the copy stored at the off-site location must be retrievable within a few hours.</p>	T	T	

Manual Security Controls, Continued

SECTION 14.O MANUAL INFORMATION SECURITY

Manual Security Controls	A	I	C
Records should be kept in a locked cabinet, room or otherwise secured storage area. Records must be secured whenever the records are not in use, not just at night. If combination or cipher locks are used, the combination/access code should be changed at least annually, or whenever there is a change in personnel allowed access to the records.	T	T	
For information with high integrity requirements, the records should be stored in a fireproof cabinet or container.		T	
The information owner must establish, for the information custodian, a list of individuals who are allowed access to the records. On a monthly basis, the owner should review and update the list.			T
A document control and tracking system must be established to maintain accountability and to further control access. This system may be automated or manual.			T
Confidential records must be kept in a locked cabinet, locked room, or otherwise secured storage areas. Locks and secure storage areas should be used whenever the records are not in use, not just at night. If combination or cipher locks are used, combinations and access codes should be changed at least annually, or whenever there is a change in personnel allowed access to the records.			T
When dealing with confidential data, weak photocopying controls can defeat strong access controls in other areas. It is counterproductive to lock everything up and log each document in and out if the person using the document is allowed to make copies at will. Only the owner, custodian, or other designated staff should be allowed to make photocopies. Photocopying by all others should be prohibited. All photocopies must be entered into the document control and tracking system under separate control numbers.			T

Manual Security Controls, Continued

Manual Security Controls	A	I	C
Confidential paper documents must be shredded or burned before being thrown away. Microfiche or microfilm must be discarded into burn bags for proper disposal.			T
Ribbons used to produce confidential documents should be placed in burn bags so that they cannot fall into the hands of an unauthorized recipient.			T

APPENDIX A

CONTINUITY OF SUPPORT AND CONTINGENCY PLANNING

[This page intentionally blank]

CONTINUITY OF SUPPORT AND CONTINGENCY PLANNING

Appendix III of OMB Circular A-130, which addresses automated information resources only, requires continuity of support plans for general support systems and contingency plans for major applications. These requirements do not extend to manual systems and therefore do not address the whole of the organization's business as often used in the context of Continuity of Operations Planning (COOP) or disaster recovery planning. However, the continuity of support and contingency plans must be coordinated with, support, and agree with the COOP planning efforts of the organization and Agency.

COOP plans are required for all Federal departments and agencies, and are especially critical for maintaining the availability of their information (both manual and automated) and information technology support for continuation of essential activities. Preparation of the plan is the responsibility of the Primary Organization Head who may delegate portions of this function to other knowledgeable individuals as long as the coordinating responsibility is retained (EPA Continuity of Operations Plan Policy, 12/20/96). Disaster recovery planning concepts (and the planning components) are most closely synonymous with the COOP planning. For example, industry use of the term disaster recovery planning suggests a comprehensive plan based on requirements of all levels of an organization, representing its major components or departments. In managing automated information resources, disaster recovery planning is used in connection with large centralized data processing facilities or installations rather than small localized LAN general support systems or widely dispersed client-server type major applications.

Typically, COOP, contingency, and continuity of support plans have three distinct areas in common concerning automated information resources:

- C Event Identification and Emergency Response Procedures: These involve identifying the types of events, likelihood of occurrence, and the actions necessary and personnel responsibilities during or immediately after an emergency to protect life and property and to minimize the impact of the emergency.
- C Backup: This area involves two components: (1) establishing a routine schedule and procedures for backing up programs and data to enable restoration of automated business functions, and (2) determining where those programs and data would run and how business functions would resume in the event of an emergency. Taken together, the two backup components ensure the continuity of information processing operations.
- C Recovery: While the backup area focuses on establishing an alternative, temporary processing capability, the recovery area focuses on restoring a permanent, ongoing capability. The process of restoring processing of both systems and applications also must concern itself with priorities for and timing of the restoration and recovery of business functions.

Contingency and continuity of support plans should be reviewed and updated on an annual basis and in coordination with COOP planning efforts. Completed plans or updates are to be forwarded to the

respective organization's SIRMO.

Steps to Develop Continuity of Support and Contingency Plans

Step 1: Determine What Constitutes a Disaster or an Event of Concern. An emergency can vary from a temporary disruption of processing to the complete destruction of the application software, facility, location, or site. Determine what kinds of events will cause: (1) limited, temporary disruption, (2) major, serious disruption, and (3) catastrophic disruption. The threats and vulnerabilities identified as part of the risk analysis can assist in this determination. It is important for distributed major applications to be coordinated with the local COOP or involved systems' continuity of support plan issues. Special consideration should be given to preventing events, to the extent possible (i.e., malicious software or intrusions which could disrupt processing). Note: Consider the above logical groupings of events during steps 2 through 4 since the magnitude of an event will generally dictate a specific set or subset of required procedures.

Step 2: Develop Emergency Procedures. Define and describe what needs to happen during and immediately after an emergency by developing procedures for:

- C Notifying personnel of the emergency
- C Responding to fire and other acts of nature
- C Evacuating the location
- C Shutting the hardware down
- C Protecting data and records
- C Contacting alternative sites for establishing temporary or permanent processing capabilities

These procedures must be written and must identify who will be responsible for what function during the emergency. All employees at the location should have an assigned function during an emergency, which may be simply to evacuate immediately and to remain home until called. It may be necessary to develop different procedures for different scenarios based on the nature and extent of the disaster or events of concern.

The procedures should be accompanied by a facility floor plan that shows the location of fire extinguishers, plastic for covering equipment, and other items useful in responding to the emergency.

Step 3: Ensure Continuity of Operations. Establish a list of items (including software, applications, and associated documentation) needed to restore business functions supported by the system or application.

Based, in part, on information manager sensitivity designations, obtain consensus and formal agreements from management (including information managers, owners, and

stewards) supported by the system and application(s). These agreements must identify the business priorities, order of importance, and timing for restoration and recovery of system processing capabilities. These items will be important in developing the plan procedures and must be approved by management and may need to be negotiated across programmatic areas. Consideration must be given to the period of time a system or application can be inoperable, the season or time of year that an event could take place, and the resulting impact on the business. Close coordination is needed between the general support system, connecting systems, users and application owners to develop a successful and workable plan. It should be noted that when a system is brought back on-line during emergency operations, the available processing capacity may be a fraction of normal capacity. Expectations should be managed.

Establish a plan for data and software backup that includes frequency of backup, a retention schedule, and an off-site location for storage. The plan should recognize that transactions that have occurred since the last data backup may be lost and may need to be re-input. Make sure the plan is responsive to program management and to any special information manager requirements.

Locate and execute an agreement for an alternative processing site to be used in the event of major or catastrophic damage. Because of cost and compatibility considerations, it is probably best to be backed-up by another EPA location.

Make sure the agreement is documented and spells out such key items as the amount of processing capability to be made available, the associated cost, and the extra supplies like blank tapes to be maintained at the backup site.

Step 4: Plan for Recovery. Develop a plan for re-establishing a permanent, ongoing processing site. If the site and its functions are of significant or critical value to the organization, identify a new site location in the event the old site cannot be rebuilt. While the staff responsible for developing the plan may not have the authority to identify a new site, the value of the location to the daily functioning of the organization and the need for a potential replacement site must still be documented and reported to management. These issues may be best addressed at the COOP planning level.

Determine how hardware supplies and other needed items will be obtained. Determine how applications will be migrated back to the original processing site or to the new site.

Step 5: Testing and Training. Test the plan. For example, confirm compatibility with the backup processing site by actually running a critical application there.

Restore applications as identified in the plan to test if adjustments to priorities are needed to ensure adequate business resumption. Testing of general systems support should be coordinated with testing of major application contingency plans where practical.

Train personnel in their emergency responsibilities.

Step 6: Prepare a Written Plan. Complete the process by formally documenting the plan. The report should include, as a minimum the following topic areas:

- C Introduction
- C Definition of Disaster and Events of Concern
- C Description of Emergency Procedures
- C Strategies for Ensuring Required Continuity of Operations
- C Plan for Recovery
- C Testing Procedures
- C Training Plan
- C Appendix Containing a Listing of Critical Information Technology Assets (include hardware, software, applications and other components, their associated supported business functions and priorities)

To the extent possible, the COOP planning format should be utilized to ensure ease of incorporation and coordination with the COOP planning process.

Step 7: Periodically Re-Test and Revise Plan. Periodically test the plan in accordance with test procedures and revise the plan and testing procedures based on the results of the test.

APPENDIX B

ANNOTATED REFERENCES

*Copies of applicable laws and regulations
may be obtained through central public
libraries or law libraries.*

[This page intentionally blank]

ANNOTATED REFERENCES

See Appendix E for a listing of document sources.

Computer Security Act of 1987. This act requires EPA to prepare security plans for sensitive applications and computer processing installations. These plans are not intended to be a detailed technical description of risks or security mechanisms; rather, the purpose of these security plans is to provide a basic overview of the security requirements of the subject application or installation and EPA's plan for meeting those requirements.

EPA Directive 2100, *EPA Information Resources Management Policy Manual*. This directive provides the policy framework for IRM within the Agency. This document provides EPA with a structure for the implementation of relevant legislation as well as policies and regulations issued by OMB and GSA—the two primary oversight agencies for Federal IRM programs. This directive establishes the authorities and responsibilities under which the IRM program functions at EPA. Detailed procedures and operating guidance are to be issued separately to supplement each of the policies. The policy manual is an EPA authoritative document (i.e., in compliance with Directive 1315) and applies to all EPA organizations, as well as the facilities, State agencies, contractors, and grantees of EPA which are involved in IRM-related activities.

***EPA Operations and Maintenance Manual*.** The ultimate purpose of this document is to help control expenditures for operations and maintenance activities and ensure that EPA uses its resources on these activities effectively and efficiently. While the *System Design and Development Guidance* document, discussed below, addresses the earlier software life cycle stages (i.e., Mission Needs Analysis; Preliminary Design and Options Analysis; and System Design, Development, and Implementation), the *Operations and Maintenance Manual* provides guidance on managing software life cycles and completes the guidance for managing the software life cycle.

***EPA Risk Analysis Guideline*.** This document provides guidance for performing risk analysis on automated information systems. The *EPA Risk Analysis Guideline* provides an approach for conducting risk analyses of the Agency's information systems. The steps in the risk analysis process include identifying and determining the value of information system assets, identifying threats and vulnerabilities, documenting the impact of threats and vulnerabilities, and identifying the most cost-effective countermeasures to protect the information systems. The *EPA Risk Analysis Guideline* provides the user with worksheets and resources tables to assist with the risk analysis process.

***EPA System Design and Development Guidance*.** This document provides a consistent focus for system development efforts which will allow both EPA program managers and OEI managers to develop and maintain the Agency's information systems cost effectively.

Federal Information Processing Standards Publication (FIPS PUB) No. 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management*. These guidelines provide a handbook for use by Federal organizations in structuring physical security and risk management programs for their ADP facilities. This publication discusses security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness, and security audit.

FIPS PUB No. 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*. These guidelines are to be used by Federal organizations to select technical and procedural methods to implement the computer security safeguards necessary for compliance with *Public Law 93-579, Privacy Act*.

FIPS PUB No. 46-1, *Data Encryption Standard*. This standard is to be used by Federal organizations when those organizations specify that cryptographic protection is to be used for sensitive or valuable computer data.

FIPS PUB No. 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification*. These guidelines are to be used by Federal organizations in the selection and evaluation of techniques for automatically verifying the identity of individuals seeking access to computer systems and networks via terminals, where controlled accessibility is required for security purposes.

FIPS PUB No. 65, *Guideline for Automatic Data Processing Risk Analysis*. This document presents a technique for conducting a risk analysis of an ADP facility and related assets. The risk analysis produces annual loss exposure values based on estimated costs and potential losses. The annual loss exposure values are fundamental to the cost-effective selection of safeguards for the security of the facility.

FIPS PUB No. 73, *Guidelines for Security of Computer Applications*. These guidelines describe the technical and managerial decisions that should be made in order to ensure that adequate controls are included in new and existing computer applications to protect them from natural and man-made hazards and to assure that critical functions are performed correctly and with no harmful side effects.

FIPS PUB No. 87, *Guidelines for ADP Contingency Planning*. These guidelines describe the issues that should be considered when developing a contingency plan for an ADP facility and provide a structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

FIPS PUB No. 102, *Guideline for Computer Security Certification and Accreditation*. This guideline is to be used by ADP managers and technical staff to establish and carry out a program and technical process for security certification and accreditation of sensitive computer applications.

Freedom of Information Act of 1974 (5 U.S.C. Section 552). The Freedom of Information Act (FOIA) requires Federal agencies to provide the ability for individuals to request information from the agencies and furnishes guidelines on how the information should be released. FOIA also stipulates the types of information that may be withheld from requesters. Other authorities, such as the *Trade Secrets Act* and the *Privacy Act*, specifically prohibit certain categories of information from disclosure. The reporting requirements established within this act include publishing information detailing the agency's organization, rules, opinions, orders, records, and procedures in the Federal Register. In addition, agencies must maintain an accounting of all requests for records that are denied and all administrative actions regarding requests for information such as, fees collected, etc.

OMB Circular A-123, *Internal Control Systems*. *OMB Circular A-123* defines the policies for internal control systems. This circular requires agencies to establish and maintain cost-effective internal controls in order to protect Government assets and resources from loss, waste, unauthorized use, or misappropriation. Internal controls are defined within the circular as the steps necessary to ensure that: (1) obligations and costs comply with applicable laws; (2) assets, funds, and other resources are safeguarded; and (3) revenues and expenditures for agency operations are recorded and accounted for. These controls must also ensure that agency programs are effective and efficient and comply with applicable laws. *OMB Circular A-123*, in conjunction with *Guidelines for the Evaluation and Improvement of and Reporting on Internal Control Systems in the Federal Government*, provides guidance and sets standards for developing the internal controls. Specifically, this circular requires agencies to develop an internal control directive and management control plan, complete and periodically update risk assessments, perform internal control evaluations, and implement corrective actions as necessary. *Circular A-123* requires agencies to prepare reports that evaluate the compliance of their internal controls to the requirements it sets forth and the compliance of all internal controls to the standards set by GAO. These reports must also state whether agency programs comply with applicable laws and document any internal control weaknesses discovered. If weaknesses are identified, the reports must also include a plan for correcting those weaknesses.

OMB Circular A-130, *Management of Federal Information Resources*. OMB Circular A-130, Appendix III details the requirements which Federal Agency information security programs must meet to provide adequate security for general support systems and major applications. OMB Circular A-130 provides definitions, lists the mandatory controls for each Federal Agency general support system or major application, assigns Federal-wide responsibilities for specific Agencies in the securing of automated information systems, and directs the correction of security deficiencies and the reporting of system security statuses. At the individual Agency activity level, the Circular stipulates for general support systems and major applications to be controlled by 1) the assignment of responsibilities, 2) the development of security plans, 3) the review of controls, and 4) the individual authorization of processing for each system and application. Within each of the mandated four controls, the Circular provides details on what is required to satisfy each control. For example, system security plans require the development and enforcement of a) rules of the system, b) training, c) personnel controls, d) incident response capability, e) continuity of support, f) technical security, and g) system interconnection.

Paperwork Reduction Act of 1995 (P.L. 104-13). The Paperwork Reduction Act of 1995 directs agencies to operate efficiently, effectively, and economically. This act emphasizes the need to protect agencies' information and information systems. With respect to computer security and privacy the act requires agencies to complete the following:

- “(1) implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency; and
- (2) assume responsibility and accountability for compliance with and coordinated management of sections 552 and 552a of title 5, the Computer Security Act of 1987 (40 U.S.C. 759 note), and related information management laws; and
- (3) consistent with the Computer Security Act of 1987 (40 U.S.C. 759 note), identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.”

Privacy Act of 1974 (5 U.S.C. Section 552). The Privacy Act of 1974 places the following requirements and restrictions on gathering and processing information: (1) Federal agencies must allow individuals access to all records pertaining to them that the agencies have gathered, used, or disseminated. The agencies must also provide the individual with a mechanism to correct or amend the records. (2) Federal agencies must obtain an individual's consent prior to using the individual's records for a purpose other than that for which it was originally gathered. The agencies must also obtain an individual's consent prior to distributing that individual's records to another agency for a purpose other than that for which it was originally intended. (3) Federal agencies must keep only necessary and lawful records; there can be no secret systems of records. A notice must be published in the Federal Register when establishing or revising a system of records. This notice must include information as to the nature of the system and the data maintained in the system and the agency's system administration policies and procedures. All records must be current and accurate for their intended use, and adequate administrative, technical, and physical safeguards must be provided to prevent misuse. (4) Federal agencies must retain and store all records required by 44 U.S.C. 3101 in accordance with the provisions of the Privacy Act. Additionally, records must be maintained for all disclosures made under the Privacy Act. Finally, (5) Federal agencies may be accountable for violations. The Privacy Act provides penalties for officers or employees of an agency who willfully violate any provisions of the act.

Trade Secrets Act of 1948 (18 U.S.C. Section 1905). This section of the U.S. Code, which is under chapter 93 of Title 18, Crimes and Criminal Procedure, prohibits any employee, officer, department, or agency of the United States from releasing confidential information except where authorized by law. In addition, this section of the code establishes penalties for the unauthorized release of this confidential information. Within section 1905, confidential information is referred to as information concerning or relating to "trade secrets, processes, operations, style of work, or apparatus or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association."

Chapter 40 Code of Federal Regulations Part 2 - Public Information (40 C.F.R. 2). This part includes policy on disclosure of EPA records, whether or not the cited under the Freedom of Information Act, 5 U.S.C. 552; identifies the categories of exempted information; procedures for confidentiality determinations; controls; penalties for disclosure; and special rules for various EPA Programs. EPA has legal and regulatory requirements to protect confidential information such as the requirements for protecting CBI at 40 CFR § 2.211. 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), contractor/sub-contractor suspension or debarment, 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.

[This page intentionally blank]

APPENDIX C

SECURITY INFORMATION RESOURCES

[This page intentionally blank]

EPA internal directives and policy manuals can be obtained by contacting the following:

EPA National Information Security Program
Office of Environmental Information
(202) 260-8671

EPA National Computer Center (NCC) Security
National Technology Services Division (NTSD)
(919) 541-4013

Security for EPA's National Security Information
Facilities Management and Services Division
Office of Administration and Resources Management
(202) 260-2013

To report information security problems, including fraud, waste, or mismanagement, call:

Personnel Security Staff
Office of Inspector General
(202) 260-4115

National Computer Center
Customer Support Service Center - Voice-Response Unit (VRU)
919-541-7862
(All computer security incidents reported to VRU will be referred to the NTSD Computer Emergency Response Team (CERT).)

Publications produced by the National Institute of Standards and Technology (NIST), such as the FIPS PUBS, can be obtained through:

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650

U.S. Department of Commerce
National Institutes of Standards and Technology (NIST)
Building 225, Room B-64
Gaithersburg, MD 20899
(301) 975-2816 (For FIPS PUBS)
(301) 975-2821 (For other NIST Publications)

Many NIST publications are available on the Internet at:
NIST Computer Security Resource Clearinghouse
<http://csrc.nist.gov/publications/welcome.html>

Copies of Federal Government documents are available through the following:

Government Printing Office
Washington, DC 20402
(202) 512-1800

Federal Depository Library System. A listing of Regional Federal Depository Libraries is available through:

Government Printing Office
Library Program Services
Washington, DC 20402
(202) 512-1014

The following organizations can supply security-related information:

ORGANIZATION	HELP AVAILABLE
<p>Computer Security Division National Computer Systems Laboratory Building 225, Room A216 National Institute of Standards and Technology Gaithersburg, MD 20899 (301) 975-2934</p>	<p>Use this contact for further information regarding NIST's computer security program, including their federal agency assistance program and their computer security bulletin board system. NIST also publishes the FIPS PUBS, many of which contain security guidelines.</p>
<p>Federal Information Systems Security Educators Association (FISSEA) Building 225, Room B154 National Institute of Standards and Technology Gaithersburg, MD 20899 (301) 975-3868</p>	<p>FISSEA operates a clearinghouse of Federal security documents; they can provide a list of relevant publications, standards, and guidelines. Many of these can be obtained in electronic or hard copy format. FISSEA also holds an annual conference where security training is provided.</p>

[This page intentionally blank]

APPENDIX D

ACRONYMS AND DEFINITIONS

[This page intentionally blank]

ACRONYMS

AA	Assistant Administrator
ADP	Automated Data Processing
CAI	Confidential Agency Information
CBI	Confidential Business Information
CERT	Computer Emergency Response Team
CO	Contracting Officer
COOP	Continuity of Operations Planning
DOPO	Delivery Order Project Officer
EPA	Environmental Protection Agency
FISSEA	Federal Information System Security Educators Association
FIFRA	Federal Insecticide Fungicide and Rodenticide Act
FIPS PUB	Federal Information Processing Standards Publication
FOIA	Freedom of Information Act
FMFIA	Federal Managers Financial Integrity Act
FMSD	Facilities Management and Services Division (Office of Administration, OARM)
GAO	General Accounting Office
GSA	General Services Administration
IRM	Information Resources Management
ISI	Information System Inventory
ISM	EPA Information Security Manual
ISO	Information Security Officer
LAN	Local Area Network
MOU	Memo of Understanding
NCC	National Computer Center
NIST	National Institute of Standards and Technology
NSI	National Security Information
OAM	Office of Acquisition Management
OAR	Office of Air and Radiation
OARM	Office of Administration and Resources Management
OC	Office of the Comptroller
OGD	Office of Grants and Debarment
OECA	Office of Enforcement and Compliance Assurance
OIG	Office of Inspector General
OEI	Office of Environmental Information
OMB	Office of Management and Budget
OMS	Office of Mobile Sources
OTOP	Office of Technology Operations and Planning
OPPTS	Office of Prevention, Pesticides, and Toxic Substance
OSWER	Office of Solid Waste and Emergency Response
OW	Office of Water

PC	Personal Computer
PO	Project Officer
RA	Regional Administrator
RACF	Resource Access Control Facility
RCRA	Resource Conservation and Recovery Act
SIRMO	Senior Information Resource Management Official
TRIS	Toxic Chemical Release Inventory Reporting System
TSCA	Toxic Substances Control Act
VRU	Voice-Response Unit
WAM	Work Assignment Manager
WIC	Washington Information Center

DEFINITIONS

Application - Per OMB Circular A-130, application means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

Availability Goal - Associated with information where the loss of the information would cause serious problems, either because it would be costly to replace the information or because it would be difficult to function without the information.

Budgetary Information Prior To OMB Release - The Agency's fiscal budget information is confidential prior to its release to Congress by the President.

Certification - Prior to the application being put into operation, an Agency official should certify that the application meets all applicable Federal policies, regulations, and standards, and that protection measures appear adequate. If the application has been in operation for a period of time, it should have been audited or reviewed and recertified within the last three years.

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.

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 effect 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.

Confidentiality Goal - Concerned with information where disclosure would be undesirable or unlawful.

Confidential Information - EPA's confidential information is information that requires protection from unauthorized disclosure under Federal statutes. Specific types of confidential information include:

- Confidential Business Information (CBI),
- Confidential Agency Information (CAI),
- Privacy Act Information,
- Some FOIA-exempt information,
- Enforcement confidential information, and
- Budgetary information prior to OMB release.

Discretionary Access Controls - A means of restricting access to objects based on the identity and need-to-know of the user, process and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. Compare with Mandatory Access Controls.

Dissemination - The active distribution of Government information to the public.

Enforcement Confidential Information - Enforcement confidential information includes privileged information that, if disclosed, would result in disruption to the legal process, or would reveal enforcement techniques.

FOIA-Exempt Information - Certain information which has been determined to be exempt from FOIA requirements due to its confidential nature. For example: FOIA-exempt information includes information regarding matters of national defense, foreign policy, or trade secrets (confidential business information) (see 40 C.F.R. 2.118).

General Support System - Per OMB Circular A-130, a 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 system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

Hacker - An individual who, without authorization, intentionally gains access to, seeks to gain access to, and/or modifies information technology resources, including data.

Information - Any communication or representation of knowledge such as facts, data, or opinions in

any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Life Cycle - The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Information Manager - The information manager is the EPA Program or Regional Office official assigned to be responsible for the management and oversight of specific information. The information manager's responsibilities may include sponsoring information, owning information, or acting as a steward for information or an application. In all cases, the information manager is responsible for ensuring that the information is managed and protected in a manner consistent with EPA's policies and standards.

Information Resource (Information Asset) - This term includes automated information systems, computerized data bases, computer programs, collections of paper records, information on microfiche or microfilm, and computer installations.

Information Resources Management (IRM) - The planning, budgeting, organizing, directing, training, and administrative control associated with Government information. The term encompasses both information and related resources such as personnel, equipment, funds, and technology.

Information Security - The precautions taken to protect the confidentiality, integrity, and availability of information. This term encompasses four different "types" of security: application security, installation security, personnel security, and security awareness training.

Information Security Officer - The primary role of an ISO is to ascertain that the security program in place for their respective organization and that, from an information security perspective, the information is properly managed. The ISO provides the SIRMO with information to determine the effectiveness and appropriateness of information security practices for systems under the purview of the SIRMO.

Information System - The organized collection, processing, transmission and dissemination of information in accordance with defined procedures, whether automated or manual. Note: An information system may consist of a major application and one or more general support systems.

Integrity Goal - Associated with information where accuracy and reliability are of particular concern. In short, integrity is concerned with protecting information from corruption.

Major Application - Per OMB Circular A-130, a 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.

Mandatory Access Controls - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. Compare with Discretionary Access Controls.

National Security Information (NSI) - 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.

Personnel Security - 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.

Physical Security - The procedures and controls to provide for the protection of personnel, facilities, materials, equipment, and documents against any threat other than overt military action.

Primary Organization Head - Primary Organization Heads include the Deputy Administrator, Assistant Administrator, Regional Administrators, the Chief Financial Officer, the Inspector General, and the General Counsel. Each Primary Organization Head is responsible for establishing an organization-wide information security program to ensure the information resources in his organization are adequately protected.

Privacy - 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.

Privacy Act Information - The Privacy Act does not apply to all personal information. It applies only to records about individuals contained in "systems of records." A "system of records" is any collection of records on individuals from which information is retrieved by the individuals' names or other personal identifiers. Examples of EPA systems of records include payroll and personnel files, Equal Employment Opportunities Commission complaint files, radon contractor files, and executive correspondence files. Records in each of these systems are retrieved by individuals' names and/or social security numbers.

Risk Analysis - A formal methodology to obtain a quantitative measurement of risk to a collection of

sensitive data and the people, information 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.

Risk Assessment - A qualitative determination of risk to a collection of sensitive data and the people, information 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.

Security Violations - Any waste, fraud, abuse, or mismanagement of information resources.

Senior Information Resources Management Official (SIRMO) - The SIRMO implements and administers their organization's information security program. The SIRMO also directs and manages information resources planning and budgeting, and ensures that information system acquisitions within their organization complies with Federal and EPA-specific policies and regulations.

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—*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*—the specific techniques and responsibilities for NSI are beyond the scope of this document.

System Manager - The system manager is a technical manager or administrator responsible for the technical operation of an automated information system. A system manager may be an application manager, an installation (facility) manager, a LAN System Manager, or a PC Site Coordinator. The system manager works with the information manager to develop and implement the specific security program consistent with the *ISM* and any organizational security policies for the information systems he/she manages.

System User - Individuals who access, receive, process, and/or store information contained in an information system (e.g., LAN/PC end user, information system developer, PC programmer, system analyst, etc).

[This page intentionally blank]

APPENDIX E

INDEX

[This page intentionally blank]

APPENDIX E

acceptable level of risk	13, 75, 76, 87, 92
access control	69-71, 100, 128
accountability	13, 16, 39, 63, 80, 85, 87, 103, 116
acquisition	37, 41, 42, 45, 47, 48, 72, 127
adequate security	13-15, 39, 87, 115, 132
application	ii, v, 3, 11, 16, 17, 22, 27, 31, 32, 39-42, 57, 62, 63, 65, 67, 69-71, 76-78, 80, 85-87, 91-93, 95, 108-110, 113, 115, 129, 131-133
assignment of responsibility	9, 84, 85, 87, 88
audit	16, 31, 39, 58, 59, 70, 71, 76, 80, 86, 87, 114
audit trail	70, 71, 80
authentication	51, 77, 79
authorization for processing	84, 88
authorized access	16, 17, 31, 44, 68
authorized use	13, 52, 53, 88
availability	v, 11-13, 15, 17, 19-21, 20, 21, 29-33, 50, 61, 62, 64, 72, 76, 78, 79, 84, 91, 93, 99-102, 107, 129, 131, 133
awareness training	ii, iv, 7-9, 38, 44, 46, 62, 72, 73, 88, 131
backup	35, 50, 63, 78, 79, 101, 103, 107, 109
CAI	24, 26, 127, 129, 130
CBI	23, 24, 61, 64, 91, 97, 117, 127, 129, 130
CERT	ii, 33, 42, 44, 46, 121, 127
Computer Security Act	8, 93, 113, 116
confidential	v, 4, 7, 11, 16, 17, 20, 23-27, 26, 27, 29-31, 45, 51, 52, 55-57, 61-64, 68, 78, 80, 91, 97-100, 103, 104, 117, 127, 129, 130, 132, 133
confidential business information	4, 7, 16, 23, 24, 97-99, 127, 129, 130
confidentiality	iv, v, 11-13, 15, 17, 19, 23-26, 30, 32, 33, 56, 62, 64, 72, 76, 77, 84, 91, 93, 99-101, 116, 117, 129, 131
contingency plan	32, 114
contingency planning	5, 31, 73, 94, 105, 107, 114
continuity of operations	39, 107, 108, 110, 127
continuity of support	5, 31-33, 58, 88, 94, 95, 105, 107, 108, 115
Contracting Officer	44, 45, 47, 68, 127
contractor	11, 39, 45, 47, 67-70, 72, 117, 129, 132, 133
control	v, 4, 7, 9, 15, 33, 39, 46, 56, 57, 64, 69-72, 75, 76, 80, 85-88, 97, 98, 100, 102-104, 113, 115, 128, 130-132
COOP	107-110, 127
costs	114, 115
cost-effective	13-15, 19, 32, 33, 79
Delivery Order Project Officer	47, 127
denial of service	16, 32, 56, 61
Directive 2100	iv, 1, 7, 113
disaster recovery	31, 107

dissemination 1, 55, 130-132

DOPO 47, 68, 71, 127

emergency response ii, 33, 44, 98, 107, 121, 127

encryption 27, 80, 114

enforcement confidential information 130

EPA Operations and Maintenance Manual 113

ethical behavior 13, 17

FIPS 51, 100, 114, 122, 123, 127

flexiplace ii, 4, 61-65, 76, 88, 95

FMFIA 40, 127

FMSD 12, 37, 42, 44, 45, 47, 127

FOIA 24, 97, 115, 127, 130

general support system 16, 32, 39, 41, 42, 44, 62, 69, 70, 76, 85, 87, 93, 95, 109, 115, 130

guideline 9, 10, 100, 113, 114

guidelines v, 7, 9, 26, 47, 52, 80, 114-116, 123

hacker ii, 29, 32, 33, 55, 56, 130

hardware v, 14, 17, 44, 50, 61-63, 78, 79, 91, 108-110, 130

incident 33, 35, 56, 94, 115

information manager ii, 2, 3, 16, 21, 42-44, 46, 48, 80, 100-102, 109, 131, 133

information resource ii, 29, 128, 131

information resources management v, 1, 37, 40, 41, 113, 127, 131, 133

information security -ii, iv, v, 1-5, 7-9, 11, 13, 19, 21, 22, 24, 37-48, 57, 67, 72, 73, 75, 80, 83-86, 89, 92-94, 97, 115, 121, 127, 131-133

information security officer ii, 2, 127, 131

information security planning iv, 7, 9, 41, 57, 80, 85, 93, 94

information security policy 1, 7, 8, 47, 83

information security program ii, iv, v, 2, 3, 7-9, 37-41, 46, 48, 67, 72, 83-85, 89, 121, 132, 133

information sensitivity 4, 11, 19, 69, 76, 77, 92

information sharing 94

information system 1, 3, 11, 14-17, 20-22, 26, 31-33, 37, 42-44, 50, 55-57, 59, 62-65, 67, 69, 70, 75, 77-79, 84, 86, 91-93, 95, 97, 113, 127, 131, 133

information technology iv, 38, 41, 51, 107, 110, 129, 130

integrity , iv, v, 11-13, 15, 17, 19, 20, 22, 23, 30-34, 51, 57, 61, 62, 64, 72, 76-78, 80, 81, 84, 91, 93, 99-101, 103, 127, 131, 133

Internet ii, 4, 17, 26, 46, 49-53, 56, 58, 64, 65, 76, 80, 88, 122

inventory 14, 43, 127, 128

IRM iv, 1, 7, 8, 7, 8, 23, 83, 113, 127, 131

IRM Policy Manual iv, 7, 8, 7, 8, 23, 83

ISM iv-vi, 1, 2, 4, 5, 8-11, 38, 41, 43, 72, 127, 133

ISO ii, 2, 3, 38, 39, 41, 43, 48, 127, 131

LAN ii, iii, 16, 34, 35, 41, 46, 63, 68, 79, 107, 127, 130, 133

least privilege 13, 16, 76, 80

APPENDIX E

life cycle	8, 11, 13, 73, 113, 131
logs	80
loss	8, 10, 11, 14, 15, 19, 21-23, 26, 29, 31, 32, 56, 71, 78, 79, 84, 99, 102, 114-117, 129, 132, 133
major application	32, 39-42, 57, 62, 69, 70, 76, 85, 87, 93, 95, 110, 115, 131, 132
managers	v, 2, 3, 15, 16, 31, 37, 41-44, 47, 48, 51, 55, 68-70, 73, 77-79, 93, 95, 97, 109, 113, 114, 127
manual information systems	1, 41, 101
medium sensitivity	80
national security information	12, 45, 47, 98, 117, 121, 127, 132
National Technology Services Division	7, 121
NCC	ii, 42, 46, 68, 121, 127
NSI	12, 44, 47, 98, 127, 132, 133
NTSD	7, 35, 42, 49, 121
OAM	37, 45, 127
OAR	99, 127
OC	127
OECA	99, 127
OEI	iv, 3, 37, 38, 45-47, 83, 113, 127
Office of Environmental Information	iv, 3, 37, 38, 46, 121, 127
Office of Technology Operations and Planning	127
OGD	37, 45, 127
OIG	37, 42, 47, 67, 68, 99, 127
OMB Circular A-130	11, 15, 31, 32, 38-40, 57, 84, 93, 107, 115, 129, 130, 132
OMS	99, 127
organizational security programs	ii, 2-4, 37, 83, 85
OTOP	127
passwords	33, 49, 58, 61, 63, 71, 79
PC	34, 35, 41, 62, 71, 128, 133
personnel screening	67-69
personnel security	ii, 4, 41, 47, 67, 69, 93, 121, 131, 132
physical security	42, 46, 47, 79, 114, 132
plan	ii-iv, 7-9, 17, 32, 38, 40-43, 57, 65, 73, 85-87, 91-93, 95, 107-110, 113-115
PO	47, 68, 128
policies	iv, v, 1, 3, 7, 17, 33, 38, 39, 44, 45, 47, 52, 84, 88, 89, 92, 98, 113, 115, 116, 129, 131, 133
policy	iv, 1, 4, 7, 8, 7-9, 12, 23, 39, 44, 47, 51, 61, 72, 75, 79, 83, 88, 91-93, 95, 107, 113, 117, 121, 130
Primary Organization Head	v, 38-40, 48, 83, 107, 132
privacy	7, 8, 11, 12, 16, 20, 24, 25, 55, 59, 92, 98, 114-116, 130, 132
Privacy Act	7, 11, 12, 16, 20, 24, 25, 59, 98, 114-116, 130, 132
Project Officer	45, 47, 127, 128
public access	iv, v, 4, 16, 19, 20, 27, 40, 49, 51, 55-59, 76, 80, 94, 95

Records Management Manual	7, 97, 98
regulations	iv, 3, 8, 9, 25, 39, 43, 46, 47, 93, 111, 113, 117, 129, 132, 133
risk	7-10, 13-15, 19, 26, 32, 33, 49, 61, 64, 65, 71, 73, 75, 76, 78, 84, 86, 87, 92, 93, 95, 100, 108, 113-116, 132, 133
risk analysis	7, 9, 10, 14, 95, 100, 108, 113, 114, 133
Risk Analysis Guideline	9, 10, 113
risk assessment	14, 65, 95, 133
risk management	13, 14, 73, 75, 93, 114
roles and responsibilities	v, 2, 4, 37, 73, 83-85, 88
rules of behavior	9, 17, 65, 86, 92, 95
safeguards	38, 41, 43, 46, 65, 91, 114, 116
screening	42, 47, 67, 68, 67-69, 68, 69, 132
security awareness	ii, iv, 7-9, 30, 31, 38, 44, 46, 62, 65, 67, 72, 73, 114, 131
security goal	17, 19-24, 76
security planning	iv, 7, 9, 27, 32, 41, 43, 57, 80, 85, 86, 91-94, 93-95
security planning guidance	iv, 7, 9, 57, 85, 93, 94
security plans	ii, iii, v, 1, 5, 7, 9, 38, 39, 41-44, 80, 84-86, 88, 91-93, 95, 113, 115
sensitive	11, 12, 19, 32, 43, 47, 67, 70, 72, 77-81, 86, 93, 95, 97, 113, 114, 132, 133
sensitivity	4, 11, 14, 15, 17, 19-22, 24, 25, 27, 43, 51, 69, 71, 76-78, 80, 83, 92, 109, 132, 133
SIRMO	ii, 2, 3, 38, 41, 42, 95, 108, 128, 131, 133
software	14, 17, 22, 30, 33-35, 39, 40, 42, 44, 48-50, 53, 55, 56, 58, 59, 61-63, 71, 78, 79, 81, 86, 108-110, 113, 130
standards	iv, v, 3, 7, 9, 17, 33, 44, 46, 47, 51, 63, 93, 97, 99, 114-116, 122, 123, 127, 129, 131
supervisor	ii, iii, 48
System Design and Development Guidance	113
system manager	42, 62, 64, 133
system user	44, 133
technical controls	15, 31, 34, 39, 42, 75, 76, 80, 84, 86, 94
test	32, 35, 50, 51, 70, 109, 110
testing	70, 71, 75, 80, 81, 80, 109, 110
threat	15, 29-33, 62, 76, 100, 132
Trade Secrets Act	115, 117
training	ii, 7-9, 17, 38, 42, 44, 46, 48, 52, 57, 62, 65, 67, 72, 73, 88, 93, 109, 110, 115, 123, 131
TSCA	4, 7, 97, 98, 128, 129
unauthorized use	v, 17, 35, 46, 115
user	16, 17, 31, 34, 44, 48, 49, 57, 59, 61, 71, 72, 77-80, 113, 129, 130, 133
violations	17, 43-48, 89, 116, 133
virus	ii, 33-35, 50, 63
vulnerability	31, 33, 58
WAM	47, 68, 71, 128
Work Assignment Manager	47, 128

[This page intentionally blank]